BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-701

30 SEPTEMBER 2005

Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ USAF/XOIW
(SMSgt Roddy Hartsook)
Supersedes AFI 10-1101, 31 May 2001

Certified by: HQ USAF/XOI (Maj Gen Sams)

Pages: 61
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 10-20, *Air Force Defensive Counterinformation Operations*, DOD Directive 5205.2, *DOD Operations Security Program*, November 29, 1999; Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01A, *Joint Information Warfare Policy*, January 2, 1996, CJCSI 3213.01, *Joint Operations Security*, May 28, 1993; and Operations Security (OPSEC) requirements for DOD Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, October 23, 2000. The reporting requirements in this publication are exempt from licensing in accordance with AFI 33-324 paragraph 2.11.1, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*. It incorporates applicable guidance from AFI 10-1101, *OPSEC* and AFI 10-2001, *Defensive Counter Information Planning, Operations and Assessment*. It applies to all Major Commands (MAJCOM), Field Operating Agencies (FOA), Direct Reporting Units (DRU) and Air National Guard (ANG). It provides guidance for all Air Force personnel and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, (will convert to 33-363) *Management of Records* and disposed of in accordance with the *Air Force Records Disposition Schedule (RDS)* located at **https://afrims.amc.af.mil/**

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

It integrates new Air Force Doctrine Document 2-5 *Information Operations* and updates the definition of OPSEC to coincide with Joint Publication (JP) 3-54, *Joint Doctrine for Operations Security*. It places related security disciplines into a table for ease of use, links OPSEC risk assessment to Operational Risk Management (ORM), introduces the OPSEC Coordinator position below wing-level, provides specific requirements for both training and assessment and defines and describes the OPSEC Survey process.

Chapter 1

INTRODUCTION

1.1. General. OPSEC is a military capability within IO. IO is the integrated employment of three operational elements: influence operations, electronic warfare operations (EW OPS) and network warfare operations (NW Ops). IO aims to influence, disrupt, corrupt, or usurp adversarial human or automated decision-making while protecting our own. Influence Operations employ core military capabilities of psychological operations (PSYOP), OPSEC, military deception (MILDEC), counterintelligence (CI) operations, public affairs (PA) operations and counterpropaganda operations to affect behaviors, protect operations, communicate commander's intent and project accurate information to achieve desired effects across the cognitive battlespace. OPSEC protects friendly operations and efforts to influence the adversary's behavior.

1.2. Definition. OPSEC is a process of identifying, analyzing and controlling critical information indicating friendly actions attendant to military operations and other activities to:

(a) Identify those actions that can be observed by adversary intelligence systems.

(b) Determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

(c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 3-54).

OPSEC is a process and not a collection of specific rules and instructions that can be applied to every operation. OPSEC must be closely integrated and synchronized with other influence operations capabilities and all aspects of the protected operations.

1.3. Characteristics of OPSEC. The goal of OPSEC is to identify information and observable activities relating to mission capabilities, limitations and intentions in order to prevent exploitation by our adversaries. OPSEC methodology provides a step-by-step analysis of our operations and behavior from an adversary's perspective, thereby assessing how vulnerabilities might be exploited. Information that adversaries need to achieve their goals constitutes critical information about our operations or programs. By identifying and protecting this critical information, the OPSEC process becomes a positive, proactive means by which adversaries are denied an important advantage.

1.3.1. Operational effectiveness is enhanced when commanders and other decision-makers apply OPSEC from the earliest stages of planning. OPSEC involves a series of analysis to examine the planning, preparation, execution and post execution phases of any activity across the entire spectrum of military action and in any operational environment. OPSEC analysis provides decision-makers with a means of weighing how much risk they are willing to accept in particular operational circumstances in the same way as ORM allows commanders to assess risk in mission planning. In fact, OPSEC can be referred to as information risk management.

1.3.2. OPSEC must be closely coordinated with other security disciplines (see **Table 1.1.**) as applicable. The primary focus of OPSEC analysis is to deny exploitation of open source information and observable activities. These sources are generally unclassified and difficult to control.

Table 1.1. Related Security Disciplines and Source Documentation

Anti-Terrorism/Force Protection Program	AFI 10-245
Communications Security User Requirements	AFI 33-211
Electronic Mail (E-mail) Management and Use	AFI 33-119
Emissions Security	AFI 33-203
Freedom of Information Act (FOIA)	DODR 5400.7/AF SUP 1999
Industrial Security	AFPD 31-6/AFI 31-601
Information Protection	AFPD 33-2
Information Security	AFPD 31-4/AFI 31-401
Network and Computer Security	AFI 33-202
Personnel Security	AFPD 31-5/AFI 31-501
Physical Security	AFPD 31-1
Privacy Act Information	AFI 33-332
Public Affairs Policies and Procedures	AFI-35-101 Chapters 15 and 18
Reporting COMSEC Deviation	AFI 33-212
Technology and Acquisition Systems Security Program Protection	AFPD 63-17
Telecommunications Monitoring and Assessment Program	AFI 33-219
Web Management and Internet Use	AFI 33-129

1.3.3. OPSEC provides a method of identifying our critical information and denying or controlling an adversary's access to that information. OPSEC enables friendly force information superiority by neutralizing adversary information collection activities.

1.3.3.1. OPSEC will be employed with other complementary IO activities to obtain maximum effectiveness. Commanders and their planners should utilize all capabilities within information operations, including OPSEC, in a synchronized effort to influence the perceptions and affect decision-making of an adversary. For example, a known OPSEC vulnerability may be used to deliver a deception message or psychological operations theme, instead of simply correcting or mitigating the vulnerability. In this case, the use of the discovered vulnerability would be considered application of the appropriate OPSEC measure.

1.4. Air Force OPSEC. The Air Force implements OPSEC in all functional areas. Commanders are responsible for OPSEC awareness throughout their organizations and for integrating the OPSEC process throughout all mission areas. Air Force commanders and decision-makers will employ OPSEC during mission planning, mission support, force execution and throughout the acquisition process. OPSEC will be incorporated into day-to-day activities to ensure a seamless transition to contingency operations.

1.4.1. OPSEC issues must be integrated into all aspects of planning and execution of all Air Force operations. OPSEC assists in the protection of Air Force capabilities and intentions by degrading an adversary's knowledge of and subsequent ability to attack our forces or counter our operations. Embedding OPSEC into campaign planning and force execution maximizes mission effectiveness.

1.4.2. OPSEC supports Air Force research, development, testing and evaluation (RDT&E) through the reduction of compromised technology and proprietary information. Acquisition organizations that fail to implement OPSEC could unintentionally reveal critical program information, ultimately increasing operational risk as potentially compromised systems are fielded.

1.4.3. OPSEC is an integral process of force protection, helping protect service members, civilian employees, family members, facilities and equipment at all locations and in all situations. Force protection relies heavily on OPSEC as a means of denying targeting information to terrorists and other adversaries. Since force protection safeguards the Air Force's most precious asset—*people*, it is critical that OPSEC be applied throughout the Air Force.

1.5. The OPSEC Process. The OPSEC process consists of five distinct steps: 1) identification of critical information, 2) analysis of threats, 3) analysis of vulnerabilities, 4) assessment of risk and 5) application of appropriate OPSEC measures (see **Attachment 1**, The OPSEC Process).

Chapter 2

AIR FORCE OPSEC PROGRAM

2.1. PURPOSE. The purpose of the Air Force OPSEC program is to provide commanders with standardized policy and to facilitate effective OPSEC programs by promoting general understanding and awareness regarding the integration and application of OPSEC. An overall Air Force OPSEC program manager (PM) is identified within the Air Staff to advise on the integration of OPSEC into service-wide efforts and to develop policy and guidance that provide coordination, training, education and recognition for Air Force-wide OPSEC programs.

2.2. ROLES AND RESPONSIBILITIES. All Air Force organizations must integrate OPSEC into their planning and develop OPSEC plans to ensure critical information and indicators are identified. The Air Force will integrate OPSEC into military strategy, operational and tactical planning and execution, all support activities, all contingency, combat and peacetime operations and exercises, communications-computer architectures and processing, weapons systems RDT&E, Air Force specialized training, inspections, acquisition and procurement, and professional military education. Although the OPSEC program helps commanders make and implement decisions, the decisions are the commander's responsibility. Commanders must understand the risk to the mission and then determine which OPSEC measures are required.

2.2.1. Headquarters, United States Air Force (HQ/USAF) Responsibilities. The Deputy Chief of Staff for Air and Space Operations (HQ USAF/XO) is the office of primary responsibility (OPR) for the Air Force IO program. HQ USAF/XO is responsible for coordinating OPSEC policy, doctrine, strategy and investment priorities with SAF/PA, SAF/IG, SAF/AQ and SAF/XC. Other offices having individual responsibilities for elements of OPSEC will coordinate with HQ USAF/XO to ensure the consistent and standardized application of OPSEC policy and guidance. HQ USAF/XO, through the Information Warfare Branch (HQ USAF/XOIW) will:

2.2.1.1. Develop OPSEC policies and guidance consistent with Joint and DOD OPSEC guidance to develop a fully capability OPSEC environment.

2.2.1.2. Designate an overall Air Force OPSEC PM.

2.2.1.3. Provide to J-3, Joint Staff, copies of all current service OPSEC program directives and/or policy implementation documents.

2.2.1.4. Support the national and DOD OPSEC programs.

2.2.1.5. Provide management, review, evaluation and assessments of the Air Force OPSEC Program.

2.2.1.6. Recommend changes to policy, plans and procedures of the DOD OPSEC Program to the Under Secretary of Defense for Intelligence.

2.2.1.7. Centrally program and manage training and funding for the overall Air Force OPSEC training program.

2.2.1.8. Utilize OPSEC training advice and services provided by the Interagency OPSEC Support Staff (IOSS) when appropriate (See Para **4.1.2.3.** for information on obtaining IOSS training.)

2.2.1.9. Provide oversight, advocacy and act as the focal point for the US Air Force Telecommunications Monitoring and Assessment (TMAP) Program.

2.2.2. Air Force MAJCOMs, FOA and DRUs. In coordination with HQ USAF/XO, commanders are responsible for OPSEC implementation, posture and operations within their commands and units. Additionally, they are responsible for enforcing OPSEC policies and directives, ensuring that OPSEC plans and programs at every echelon are supported by the existing intelligence organizations/infrastructure at those levels. At the base/installation level, FOAs and DRUs will comply with host MAJCOM and Wing guidance. MAJCOMs, ANG, FOAs and DRUs will develop effective OPSEC programs that meet the specific needs of their assigned mission and accomplish the following:

2.2.2.1. Designate a primary and alternate PM, in writing. The PM may be military or DOD civilian. MAJCOMs are strongly encourage to have a full-time OPSEC PM due to the critical nature of OPSEC with respect to air and space operations. Forward copy of the appointment letter to HQ USAF/XOIWS.

2.2.2.2. Develop an OPSEC program IAW policy and guidance issued by HQ USAF/XO and ensure subordinate organizations integrate OPSEC into day-to-day operations. Ensure OPSEC is integrated with other IO activities.

2.2.2.3. Program fund for all OPSEC training through established budgeting and requirements processes. All OPSEC PMs will submit annual budget requirements through their respective commands to Air Staff for inclusion into the Air Force Program Objective Memorandum (POM) process. OPSEC capabilities and solutions requirements will be identified through the IO Capabilities Plan, then submitted to the POM process through respective MAJCOM or Program leads.

2.2.2.4. Provide coordination across organizational boundaries as necessary (both vertically and horizontally) to facilitate consistent application of OPSEC throughout the command.

2.2.2.5. Ensure all subordinate units are identifying critical information for each operation, activity and exercise whether it be planned, conducted, or supported.

2.2.2.6. Ensure all subordinate units are controlling critical information and indicators.

2.2.2.7. Ensure all subordinate units plan, exercise and implement OPSEC measures as appropriate.

2.2.2.8. Ensure OPSEC considerations are integrated into the acquisition cycle. Ensure OPSEC considerations are included in Initial Capabilities Documents, Capability Development Documents and inputs to the combatant commanders' Integrated Priority Lists.

2.2.2.9. Develop and cultivate the intelligence and CI relationships necessary to support OPSEC programs.

2.2.2.10. IAW AFI 33-129, ensure OPSEC considerations are included in annual unclassified public web page reviews and in the approval process for posting new data to the web.

2.2.2.11. Ensure OPSEC considerations are included in PA's review and approval process for the publishing or releasing of information to or that may be viewed by the public, i.e. base newspapers, safety magazines, flyers, web pages, television interviews and information for news articles.

2.2.2.12. Ensure mission-oriented OPSEC education and awareness training is provided to all personnel within 90 days of initial assignment and then annually thereafter.

2.2.2.13. Ensure training of OPSEC PMs at wing-level and above is accomplished within 90 days of appointment, or by the next available class.

2.2.2.14. Will forward a consolidated self-assessment report to the Air Force OPSEC PM (HQ USAF/XOIW) NLT 15 Nov each year. This report will contain training metrics of initial and refresher training for all subordinate units, the number of vulnerability reports forwarded to the IO Threat Analysis Center, number and type of survey/assessments received by subordinate units (command survey, TMAP support, Multi-Discipline Vulnerability Assessment (MDVA), and any other information deemed of OPSEC importance.

2.2.2.15. Ensure OPSEC vulnerability reports are forwarded to HQ AIA's IO Threat Analysis Center in a timely manner. See **Attachment 4** for sample vulnerability report format and addressing instructions.

2.2.2.16. Develop policy and issue implementing supplements or other guidance as required.

2.2.2.17. Prioritize and consolidate vulnerability assessment requirements (i.e. MDVAs and/or formal surveys) for NAFs, wings and subordinate units. Forward requirements to ACC/DOZ for scheduling.

2.2.2.18. Serve as the focal point for TMAP operations.

2.2.3. Air Combat Command (ACC). As the Combat Air Force lead for IO, ACC will:

2.2.3.1. Consolidate OPSEC requirements into the Air Force IO Capabilities Plan.

2.2.3.2. Develop Air Force OPSEC tactics, techniques and procedures (TTP).

2.2.3.3. Integrate OPSEC into the Air Operations Center (AOC) construct.

2.2.3.4. Provide OPSEC support assessment capabilities to include TMAP, MDVAs, formal surveys and AFWRAC capabilities for the Air Force.

2.2.3.5. Develop, maintain, program for and provide Air Force OPSEC PM and Coordinator training.

2.2.3.6. Coordinate with the Air Force Experimentation Office to incorporate Air Force OPSEC initiatives into Joint/Air Force experimentation and traditional and spiral development acquisition activities.

2.2.3.7. Ensure OPSEC vulnerability reporting is included in Influence Operations fused analysis by the IO Threat Analysis Center.

2.2.3.8. Provide OPSEC Advisory reporting to the Air Force through the IO Threat Analysis Center.

2.2.4. Air Material Command (AMC). As the Mobility Air Force lead, AMC will:

2.2.4.1. Consolidate OPSEC requirements into the Air Force IO Functional Area Plan

2.2.4.2. Lead centralized management of OPSEC functions and the establishment and integration of OPSEC in Mobility Air Force operations.

2.2.4.3. Develop Mobility Air Force OPSEC TTP.

2.2.4.4. Integrate OPSEC into AMC's AOC, the Tanker Airlift Control Center.

2.2.4.5. Integrate OPSEC into all AMC plans and activities as outlined in Para **3.1.3.**

2.2.5. Air Force Material Command (AFMC). AFMC will ensure OPSEC is integrated into all RDT&E efforts and OPSEC principles are applied throughout the life cycle of all weapon systems.

2.2.6. Air Education and Training Commander (AETC). AETC will:

2.2.6.1. Provide OPSEC orientation for all new Air Force accessions. The block of training must include a basic overview of the OPSEC process, the purpose, history and value of OPSEC.

2.2.6.2. Reinforce OPSEC doctrine and capabilities during professional military education at all levels.

2.2.6.3. Incorporate OPSEC concepts and capabilities into specialized courses, such as the Contingency Wartime Planning Course, Joint Air Operations Planning Course and the Information Warfare Application Course. These courses will include command responsibilities and responsibilities of OPSEC planners in Joint Force Command IO Cells and MAJCOMs.

2.2.6.4. Incorporate and reinforce OPSEC concepts and capabilities in all technical and specialty school programs.

2.2.6.5. In conjunction with HQ USAF/XOIW, establish a validation process for all AETC OPSEC training programs used in accession, professional military education, technical and specialty training courses.

2.2.6.6. Develop and sustain computer-based training for Air Force-wide newcomers and annually recurring requirements.

2.2.7. Air Force Office of Special Investigations (AFOSI). AFOSI will:

2.2.7.1. Provide OPSEC PMs, coordinators and unit commanders with AFOSI Local Threat Assessments and Multi-discipline Counterintelligence (MDCI) Threat Assessments.

2.2.7.2. AFOSI detachment commanders will assist their local commanders with access, as necessary, to threat information from sources outside the Air Force.

2.2.7.3. Provide HUMINT Vulnerability Assessment in support of MDVAs and command surveys.

2.2.8. US Air Force Academy. The US Air Force Academy will provide OPSEC orientation for all Air Force cadets. The training must include a basic overview of the OPSEC process, the purpose, history and value of OPSEC.

2.2.9. The Secretary of the Air Force Chief Information Officer (SAF-CIO). The Secretary of the Air Force Office of Warfighting Integration and Chief Information Officer (SAF/XC) is the OPR for information assurance policy, guidance and operational oversight. SAF/XC is responsible for ensuring that AF OPSEC principles and practices are correctly reflected in the AF Enterprise Architecture. SAF/XC is also responsible for ensuring interoperability of information warfare systems and concepts.

2.2.10. The Office of the Secretary of the Air Force, Public Affairs (SAF/PA). SAF/PA is the OPR for Public Affairs Operations.

2.2.11. The Assistant Secretary of the Air Force, Acquisition (SAF/AQ). SAF/AQ is the OPR for Air Force Acquisition and RDT&E.

2.2.12. Academy of Military Science (AMS). AMS provides OPSEC orientation for all new Air Force accessions. The block of training must include a basic overview of the OPSEC process, the purpose, history and value of OPSEC.

2.3. OPSEC REPORTING. The Air Force OPSEC program's reporting requirements include two types of time-sensitive reports:

2.3.1. OPSEC Vulnerability Reports. An OPSEC vulnerability report identifies a disclosure of critical information or provides the identification of OPSEC indicators that could jeopardize ongoing or planned operations. These reports may warrant dissemination beyond the particular unit to enable damage control measures to minimize potential exploitation by adversaries and ensure implementation of OPSEC measures. This reporting is not intended to assign blame or initiate punitive action, but rather to highlight potential vulnerabilities, identify trends and improve the Air Force' OPSEC posture. OPSEC PMs and coordinators are the focal points for ensuring commanders are advised of local OPSEC vulnerabilities and the importance of reporting them as part of the Air Force' overall IO and OPSEC program. Reports will be submitted to the IO Threat Analysis Center OPSEC Section who will make fused reports available to MAJCOM OPSEC PMs and other entities as necessary. Vulnerability Reports can be submitted by MAJCOM or Wing level PMs, TMAP teams, MDVA teams, Survey Teams or the Web Risk Assessment units that identify a possible disclosure of critical information or an OPSEC indicator that jeopardizes the organization's operations. Any other individual or organization that identifies a possible vulnerability should forward through their chain of command to those entities authorized to validate and submit Vulnerability Reports (See **Attachment 4** instructions for completing and forwarding a report).

2.3.2. OPSEC Advisory Reports. An OPSEC Advisory Report provides advance notification of a potential threat to operations. Examples include flight paths of foreign aircraft over US territory, location of foreign naval vessels with collection capabilities and projected commercial satellite exploitation. While not the only source for Advisory Reports, HQ AIA IO Threat Analysis Center provides these reports as required. OPSEC PMs must review OPSEC Advisory Reports and ensure commanders and subordinate organizations are informed.

2.4. AIR FORCE OPSEC AWARDS PROGRAM. The annual Air Force OPSEC Awards Program provides recognition of Air Force OPSEC professionals and is a top priority for the Air Force OPSEC program. This awards program runs concurrently with the National OPSEC Awards Program conducted by the IOSS. Although the Air Force will only select one winner per category, all MAJCOM nominations will be forwarded to the IOSS to compete in their national-level awards program. Awards announcement and solicitation will be forwarded annually; however, submissions will generally be due to HQ USAF/XOIWS NLT 1 Dec each year. The program runs on a Fiscal Year basis. Categories include:

2.4.1. Air Force OPSEC Organizational Achievement Award. The Air Force OPSEC Organizational Achievement Award is in recognition of outstanding organizational accomplishments during the award period. The nomination narrative should be no longer than three pages, single-spaced and should describe the specific accomplishments of the nominated organization. The criteria considered for both categories include, but are not limited to, the following:

2.4.1.1. Evidence of organizational ability to identify and solve significant OPSEC problems, threats, or vulnerabilities.

2.4.1.2. Creation or development of innovative programs for OPSEC training, education or awareness; and,

2.4.1.3. Mission accomplishments and successes at the organizational-level resulting from the application of OPSEC.

2.4.2. Air Force OPSEC Individual Achievement Award. The Air Force OPSEC Individual Achievement Award is in recognition of outstanding individual accomplishments during the award period. The nomination narrative should be no longer than three pages, single-spaced and should describe the specific accomplishments of the nominee. The criteria considered includes, but is not limited to, the following:

2.4.2.1. Evidence of individual ability to identify and solve significant OPSEC problems, threats, or vulnerabilities.

2.4.2.2. Demonstration of outstanding leadership and knowledge in the application of OPSEC.

2.4.2.3. Innovative and creative use of resources (personnel, fiscal, or facilities) to successfully accomplish OPSEC-related goals and missions.

2.4.3. Air Force OPSEC Multimedia Achievement Awards. The Air Force OPSEC Multimedia Achievement Award is in recognition of outstanding multimedia accomplishments during the award period. This award is designed to stimulate the development and distribution of OPSEC-related education and awareness materials. The two Air Force OPSEC Multimedia Achievement Awards categories are Electronic Media Award (e.g. videotapes, CDs); and, Print Media Award (e.g. posters, brochures). Each electronic and print nomination should include a narrative not longer than two pages, single-spaced, describing the media, its use (i.e. training, awareness, etc.), benefits and what was accomplished through use of media. Posters must be mounted on poster board and be no larger than 30 x 40 inches. If possible, submit at least seven copies of the nominated videotapes or CDs. The criteria considered for both categories include, but are not limited to, the following:

2.4.3.1. Presents a valid educational, training, or OPSEC awareness theme or message.

2.4.3.2. Be of artistic value and visual impact.

2.4.3.3. Be completed during the fiscal year being evaluated.

2.4.3.4. Include a certification that products contain no copyright material and, if applicable, are for in-house use only.

2.4.4. Air Force OPSEC Literature Achievement Award. The Air Force OPSEC Literature Achievement Award recognizes outstanding literary accomplishments during the award period. Nominations may be made for an individual or for a body of work (e.g., a series of OPSEC-related articles). The submission must be a minimum of 5,000 words. Documents must be composed in Microsoft Word or equivalent, single-spaced, with 1” margins, using Times New Roman 12 point font. A hard copy and an electronic copy (either disk or CD ROM) are required. Topics or subjects suitable for submission include, but are not limited to, the following:

2.4.4.1. Technical aspects of any or all components of the OPSEC Process. Relationship between 1) OPSEC and Information Operations/Assurance, 2) Security and or intelligence issues, 3) National Security, 4) Risk Management and 5) Other Related Disciplines.

2.4.4.2. Lessons learned derived from OPSEC.

2.4.4.3. Impact of an OPSEC program and/or dissemination of the article or its circulation in a publication.

2.4.4.4. Presents a valid educational, training, or OPSEC awareness theme or message.

2.4.5. Award submission procedures. MAJCOMs, ANG, FOAs and DRUs will submit awards packages to HQ USAF/XOIWS, 1400 Key Blvd, St. 300, Rosslyn, VA 22209, by 1 December of each year. Submissions can be made electronically and should include a cover letter and nomination letter for both the Air Force-level awards and the IOSS program awards. More information concerning IOSS requirements can be found at **www.ioss.gov**.

Chapter 3

UNIT OPSEC PROGRAM

3.1. Purpose and Composition. Unit OPSEC programs support the commander's efforts to accomplish a successful and effective mission. Each program is composed of an OPSEC PM or coordinator, OPSEC plans, funding, training, assessments and feedback. Unit OPSEC programs must have the following critical aspects: commander involvement, operational focus, integration, coordination and self-assessment.

3.1.1. Commander Involvement. Commanders are responsible for ensuring OPSEC is integrated into day-to-day operations. Commanders may delegate authority for OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of OPSEC measures.

3.1.2. Operational Focus. The OPSEC program is an operations program and its goals are information superiority and optimal mission effectiveness. The emphasis is on OPERATIONS and the assurance of effective mission accomplishment. The unit PM and Coordinator should reside in the operations or plans element of an organization or report directly to the unit commander to ensure effective implementation across organizational and functional lines. However, for those units with no traditional operations or plans element, the commander must decide the most logical area to place management and coordination of the unit's OPSEC program while focusing on operations and the mission of the unit.

3.1.3. Integration. PMs and coordinators will integrate OPSEC into all organizational plans and activities. Staff elements and supporting organizations will ensure OPSEC is appropriately incorporated at the earliest possible time into all operations plans (OPLANs), concept plans (CONPLANs), concept of operations (CONOPs), operations orders (OPORDs), exercise plans, Initial Capability Documents (ICD), Capability Development Documents (CDD), Initial Requirement Documents (IRD), program protection plans (PPP), operating procedures and other plans and activities to ensure consistent control of critical information and OPSEC indicators. All applicable contracts, Statements of Work (SOW), Requests for Proposals (RFP) and similar documentation will contain specific statements or requirements that address security criteria for protecting critical information and OPSEC indicators. All OPSEC PMs and coordinators will add an OPSEC section to each respective annex to all organizational plans. The appropriate functional area OPSEC PM or coordinator will evaluate all appropriate contractual documents regarding OPSEC and will work with the local contracting office to ensure the intent of the program is met.

3.1.3.1. OPSEC must be an integral part of an overall IO effort. This applies to other IO and Influence Operations functions that also protect friendly information and that may influence the adversary's decision-making process. For example, integration of OPSEC and Public Affairs is particularly important as the need to protect critical information must be balanced against the desire to provide information to the public. The PM or coordinator will maintain copies of all applicable Public Affairs guidance and ensure the Public Affairs office is aware of critical information elements.

3.1.3.2. OPSEC is integrated into the AOC through the IO Team. IO Team OPSEC coordinators/planners work within the AOC to ensure planning and execution of air, space and IO incorporate OPSEC. IO Team OPSEC coordinators/planners work with the rest of the IO Team to integrate OPSEC with other IO activities. When an AOC is formed, IO Team OPSEC coordinators/planners become the focal point for integrating the activities of supporting commands OPSEC PMs and coordinators. This ensures the commander, Air Force forces (COMAFFOR) has a coherent OPSEC effort across all Air Force units.

3.1.3.3. Each unit (MAJCOM and below) will have a written OPSEC plan. OPSEC PMs and coordinators will use AFTTP 3-1, Vol 36 (SIPRNet: **http://iwtactics.afiwc.aia.Kelly.af.smil.mil/home**) when developing these plans since this TTP provides the "how to" for planning and executing IO and OPSEC. All OPSEC plans will utilize the plan format listed below:

OPSEC PLAN FORMAT

1. References

2. General Mission/Program Description

3. Security Responsibilities

4. Critical Information List (CIL)

5. Indicators

6. Threat

7. Vulnerabilities

8. Measures and Risk Assessment

9. Public Affairs

10. Training

11. Supporting Units/Associated Programs

3.1.4. Coordination. OPSEC must be coordinated with IO and all the other elements of Influence Operations. Coordination across functional and organizational lines facilitates OPSEC planning and enhances the effectiveness of OPSEC measures.

3.1.4.1. Organizations preparing to deploy must follow the Theater OPSEC plan and coordinate OPSEC with the gaining command's OPSEC PM, coordinator, or IO Team OPSEC Planners.

3.1.5. Self-Assessment. PMs and coordinators will accomplish a self-assessment in accordance with **Chapter 5**, NLT 30 September of each year.

3.2. OPSEC PMs. OPSEC PMs and Alternates will be assigned at wing-level or wing-equivalent and above. Organizations at wing or wing-equivalent level (and above) must appoint an OPSEC PM and Alternate, in writing. The wing or wing-equivalent level PM can come from any organizational level the commander deems appropriate. For example, the wing PM may actually be assigned at the Operations Group level, but performs OPSEC PM duties in direct support of the entire wing. Letters of appointment must be forwarded to respective MAJCOM OPSEC PMs or the HQ USAF OPSEC PM, as appropriate. The respective commander or HHQ directorate will sign appointment letters. Units below that level that do not have OPSEC PMs must assign an OPSEC Coordinator and Alternate to work with PMs at wing and higher headquarters (HHQ). OPSEC PMs at the MAJCOM level should be assigned for a minimum of 18 months. The OPSEC PM requires a security clearance appropriate to the mission and function of the organization, but no lower than Secret. Wing or wing-equivalent (and above) PMs require SIPRNET access to access OPSEC Advisory Reports, whether in their work center or from another terminal on the installation. All OPSEC PMs must establish NIPRNET and SIPRNET organizational accounts. Wing or wing-equivalent OPSEC PMs may also serve as the lead Influence Operations and Information Operations Manager. Wing OPSEC PMs will coordinate OPSEC with tenant unit OPSEC PMs and/or Coordinators. Tenant OPSEC PMs and Coordinators will closely coordinate and integrate with host wing OPSEC initiatives; however, administrative oversight of the tenant unit's program still resides with their respective parent MAJCOM. If the host organization has an OPSEC working group, the tenant unit PM or Coordinator will seek representation in it.

3.2.1. OPSEC PM duties include, but are not limited to:

3.2.1.1. Develop, coordinate and manage the OPSEC Program, Program Plan and implementation throughout his/her organization.

3.2.1.2. Incorporate OPSEC into organizational plans, exercises, activities and command-to-command agreements.

3.2.1.3. Incorporate OPSEC lessons learned from unit operations and exercises as well as other operations and exercises into the unit's planning process. Forward lessons learned to appropriate depositories.

3.2.1.4. Oversee development and implementation of the commander's OPSEC policy and CIL.

3.2.1.5. Develop procedures to ensure critical information and OPSEC indicators are controlled.

3.2.1.6. Ensure OPSEC reviews are conducted on all web pages annually or prior to the information being placed, updated, or modified on the web page.

3.2.1.7. Ensure OPSEC considerations are included in PA's review and approval process for the publishing or releasing of information to or that may be viewed by the public, i.e. base newspapers, safety magazines, flyers, web pages, television interviews and information for news articles.

3.2.1.8. Ensure OPSEC reviews consider the proliferation of internet/web-based bulletin boards and logs (blogs) and evaluate the risk presented by web content in annual OPSEC assessments.

3.2.1.9. Ensure OPSEC is integrated into Information Operations, Influence Operations and other supporting capabilities.

3.2.1.10. Provide management, development and oversight of appropriate OPSEC training and conduct training as required.

3.2.1.11. Ensure annual OPSEC self-assessments are conducted by subordinate units and results forwarded to next HHQ by 15 October of each year.

3.2.1.12. Chair OPSEC Working Group (OWG) (normally wing-level) consisting of appropriate IO and security disciplines and applicable supporting organizations.

3.2.1.13. Coordinate and facilitate OPSEC assessments IAW **Chapter 5**.

3.2.1.14. Submit OPSEC vulnerability reports IAW **Chapter 2**.

3.2.1.15. Ensure OPSEC is integrated into all acquisition programs and contractor support documents/agreements.

3.2.1.16. Conduct Staff Assistance Visits (SAV) to all subordinate units as required or requested.

3.2.1.17. Serve as the focal point for TMAP (AFI 33-219).

3.3. OPSEC Coordinators. OPSEC Coordinators and Alternates will be assigned for each subordinate unit under wing or wing equivalent level. MAJCOM, ANG, FOA and DRUs also require coordinators within HQ directorates, as appropriate. Letters of appointment must be forwarded to respective HHQ OPSEC PM. The respective commander or MAJCOM directorate will sign appointment letters. All OPSEC coordinators will maintain an appropriate clearance, but a minimum of Secret is required. If possible, OPSEC coordinators should not have any other additional duties. Tenant unit OPSEC coordinators will closely coordinate and integrate with host wing OPSEC initiatives; however, administrative oversight of the tenant unit's program still resides with their respective parent MAJCOM. If the host wing has an OPSEC working group, the coordinator will seek representation in it.

3.3.1. OPSEC Coordinator duties include, but are not limited to:

3.3.1.1. Implement and execute OPSEC utilizing commander and HHQ OPSEC PM policy and guidance

3.3.1.2. Incorporate OPSEC into organizational plans, exercises and activities.

3.3.1.3. Submit lessons learned from operations and exercises to respective wing or HHQ OPSEC PM as appropriate.

3.3.1.4. Oversee development and implementation of commander's OPSEC policy and CIL.

3.3.1.5. Develop procedures to ensure critical information and OPSEC indicators are identified and controlled.

3.3.1.6. Ensure OPSEC reviews are conducted on all web pages annually or prior to the information being placed, updated, or modified on the web page.

3.3.1.7. Conduct OPSEC reviews of information submitted for publication or release to the public, i.e. base newspapers, safety magazines, flyers, web pages, television interviews information for news articles.

3.3.1.8. Provide management of unit's OPSEC training and ensure the performance of initial OPSEC training upon arrival of newly assigned personnel and annual refresher training thereafter.

3.3.1.9. Conduct and report annual OPSEC self-assessments to respective wing or HHQ OPSEC PM as appropriate NLT 15 October of each year IAW **Chapter 5**

3.3.1.10. Participate in OWG as required.

3.3.1.11. Utilize assessment results to correct discovered vulnerabilities and aid organization OPSEC awareness efforts.

3.3.1.12. Submit OPSEC vulnerability reports IAW **Chapter 2**.

3.3.1.13. Integrate OPSEC into all acquisition programs and contractor support documents.

3.3.1.14. Coordinate with appropriate organizations and wing/wing-equivalent senior leadership to resolve/mitigate Web Risk Assessment, TMAP, MDVA and other OPSEC assessment findings as required.

3.3.1.15. Serve as the unit focal point for TMAP (AFI 33-219).

3.4. OPSEC Planners. OPSEC planners are personnel who accomplish the duties of an OPSEC Coordinator, but have received specialized planning training (i.e. IO Integration Course, AOC Field Training Unit). OPSEC Planners normally reside within the Information Warfare Flight construct. When employed within the AOC, OPSEC Planners function as part of the IO Team.

3.5. The OPSEC Working Group. An OWG will be established at wing- (or wing equivalent) level. In addition, an ad-hoc OWG should be established for any large-scale operation or exercise. At the wing- (or wing equivalent) level, the OPSEC PM will chair the OWG and report directly to the commander. The OWG will ensure the timely and efficient review of activities and future plans. The OWG will also integrate OPSEC into all organization planning and operational processes. The OWG composition will vary depending on various projects or activities being performed. At a minimum, the OWG should include a representative from each exercise or operation, as well as any direct units associated with an exercise or operation. Recommended members include the MILDEC Officer, PSYOP Officer, Senior Intelligence Officer, PA Officer, Force Protection Officer, Information Assurance Officer, Local AFOSI Detachment and all subordinate OPSEC Coordinators. The OWG force protection member may be either a representative from the Wing Anti-terrorism Office (ATO) or installation Security Forces (SecFor). The OWG should compliment installation anti-terrorism working groups (formerly Threat Working Groups), force protection working groups and critical infrastructure working groups.

Chapter 4

AIR FORCE OPSEC EDUCATION AND TRAINING

4.1. Purpose. Initial and annual OPSEC training provides Air Force personnel (military and civilian) with general knowledge of the OPSEC process. Air Force contractors who have access to mission critical information will also receive the same training. Training ensures Air Force personnel and supporting contractors understand their individual responsibilities, realize the positive benefits of proper OPSEC and gain a greater appreciation of how the Air Force uses OPSEC measures to minimize the exploitation of critical friendly information. Formal OPSEC training for those assigned as PMs or Coordinators is accomplished through ACC's Air Force Information Warfare Center (AFIWC) and provides more in-depth training designed to ensure proper management and execution of organizational OPSEC programs.

4.1.1. OPSEC Education is a Continuing Requirement. Training must be provided to personnel upon their initial entrance/accession into military service (AMS, BMTS, ROTC, OTS, Air Force Academy, etc.) and upon assignment to new organizations. Contractors must ensure employees receive OPSEC training within 90 days of initial assignment to a contract with OPSEC requirements and civilian personnel must receive OPSEC training upon accession and within 90 days of assignment to a new organization. OPSEC PMs and Coordinators will track and document the completion of training for all military, civilian and contractor personnel. General guidelines for this training follow:

4.1.1.1. Accession training will provide a brief overview of the OPSEC process, the importance of understanding critical information and the general adversary threat.

4.1.1.2. Unit-specific OPSEC education will be provided as part of in-processing for all new personnel and before individuals receive access to mission critical information. The purpose of unit OPSEC education is to ensure personnel are familiar with potential threats related to the unit, critical information for the mission it supports, job specific OPSEC indicators and the OPSEC measures they will execute. Briefings to new personnel should include duty related critical information, the intelligence threat to the mission supported and individual responsibilities. Refresher training will occur during the AEF training cycle for those units with AEF tasking or at least annually for those without AEF commitments. Refresher training must include, as a minimum, updated threat information, changes to critical information and new procedures and/or OPSEC measures implemented by the organization.

4.1.1.3. OPSEC Training Documentation. All unit OPSEC Coordinators will track initial and refresher training and report training metric results to respective HHQ OPSEC PM for inclusion in their annual OPSEC self-assessment report. Wing level OPSEC PMs will forward their combined results to their respective HHQ PM who will include results in their annual reports to HQ USAF/XOIW. Wing, MAJCOM, FOA and DRU PMs are also responsible for the reporting of command/wing staff personnel training statistics.

4.1.2. OPSEC Training Requirements for PMs and Coordinators.

4.1.2.1. Formal OPSEC Training. This level of training is required for all individuals designated as OPSEC PMs at wing-level (or wing equivalent) and above, IO Red Team members who conduct MDVAs and those who conduct formal OPSEC surveys and IG inspections.

4.1.2.2. For OPSEC PMs above the wing level, OPSEC training must be completed within 90 days of appointment in either the next available Air Force OPSEC course, through the IOSS DOD OPSEC Course or an equivalent course; however, the Air Force course is the preferred method. For PMs at the wing (or wing-equivalent) level in-residence formal training must be scheduled within 90 days of the assignment. In addition, all OPSEC Planners require this training. Coordinators below wing-level are strongly encouraged to attend formal Air Force OPSEC training; however, coordinators below wing-level should seek training directly from their wing-level PM. Submit waivers for extreme circumstances through parent MAJCOM, ANG, FOA, or DRU OPSEC PM to HQ AF/XOIWS for approval. Program managers must maintain general awareness of current OPSEC related events and seek continuation training at every opportunity. OPSEC PM training is unit-funded.

4.1.2.3. Requests for OPSEC training in formal Air Force courses must be forwarded through wing PMs to their respective MAJCOM, ANG, FOA, or DRU OPSEC PM, who will prioritize their command's requirements and submit them to the AFIWC OPSEC Course Registrar at the 39 IOS, Hurlburt Fld FL. Requests for IOSS courses may be sent directly to the IOSS (**www.ioss.gov**). All OPSEC PMs will advise their respective HHQ when training has been completed.

4.1.2.4. Direct liaison authority between AFIWC and MAJCOM, ANG, FOA and DRU OPSEC PMs is permitted to support curriculum development and management.

Chapter 5

ASSESSMENTS

5.1. Purpose. OPSEC assessments are accomplished to gauge the overall health of the OPSEC program, to examine actual practices and procedures and to identify new or previously undiscovered vulnerabilities. Commanders, PMs and coordinators use assessment results within the risk management process to implement protective measures and improve the OPSEC posture of the unit/activity.

5.2. Scheduling. MAJCOM PMs will coordinate with their wings and subordinate units to schedule assessments. PMs will then validate and prioritize their units based on a priority system taking into account the unit's mission criticality, threat (based on inputs from intelligence and counterintelligence sources) and operations tempo. Finalized lists will be forwarded through ACC/DOZ for scheduling (or other organization as ACC determines). Because ACC assessment assets are limited, PMs will work closely with scheduling agencies to resolve tasking conflicts. If conflicts cannot be resolved, HQ AF/XOIW will be the determining authority. Wing commanders entering an Air Expeditionary Force (AEF) cycle are highly encouraged to request a MDVA or OPSEC Survey just before the beginning of their AEF cycle and the highest priority will be given to fulfilling their requests.

5.3. Methods. There are several types of assessments available to OPSEC PMs or coordinators to gauge the effectiveness of their program. The nature of the assessment depends on the unit's mission criticality, availability of resources and commander guidance as illustrated in **Table 5.1.**

5.3.1. Program Self-Assessment. Unit PMs and coordinators will conduct annual self-assessments to ensure the health of their program, evaluate compliance with applicable policies and to identify shortfalls and vulnerabilities. **Attachment 2** contains a sample self-assessment checklist that can be modified to suit specific unit/activity needs.

5.3.2. Web Risk Assessment. Web risk assessment is conducting ongoing OPSEC analysis of content and data resident on Air Force owned, leased, or operated publicly accessible and NIPRNet websites. Web risk assessment follows guidance contained within AFI 33-129, *Web Management and Internet Use and* AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*. Web risk assessment is an integral portion of the Air Force's TMAP. The goal of Web risk assessment is to improve the Air Force OPSEC posture and identify critical information available for adversary exploitation. Web risk assessment reviews and evaluates findings, reports to the unit for correction and forwards results to the IO Threat Analysis Center for fused analysis and dissemination.

5.3.3. Telecommunications Monitoring and Assessment Program (TMAP). TMAP involves the collection and analysis of unsecured and unprotected voice, fax, data (networks and wireless devices) and other electronic transmissions or communications systems to evaluate an organization's OPSEC posture and determine the amounts and types of information available to adversary collection entities. Telecommunications monitoring is accomplished only within certain legal parameters and may only be performed by authorized agencies as outlined in AFI 33-219, *Telecommunications Monitoring and Assessment Program* (TMAP). Telecommunications monitoring is normally conducted upon request of an appropriate authority (wing/CC), provided assets are available. The analysis and recommendations are formally reported to the requesting authority. Telecommunications monitoring can be conducted as part of a survey, an MDVA, or a stand-alone assessment. Units should have their telecommunications assessed at least biennially (every two years). Commanders can request a TMAP mission by contacting their Wing, MAJCOM, ANG, FOA or DRU PM.

5.3.4. Staff Assistance Visit (SAV). OPSEC PMs at the wing-level should conduct annual SAVs of their subordinate units. SAVs check for program compliance (i.e. Special Interest Items, Air Force Instructions, MAJCOM policies, etc.), identify and resolve shortfalls and provide guidance to PMs/ Coordinators as required. SAVs also identify and share “best practices” throughout their respective command.

5.3.5. Survey. The OPSEC survey is a systematic process to examine the actual practices and procedures employed by an activity or operation to achieve its goals. The methodology consists of using a team to look at an activity through the eyes of an adversary to determine if critical information may be inadvertently disclosed through the performance of normal organizational functions. The primary purpose is to evaluate and improve organizational effectiveness and control the vulnerabilities of friendly actions or information. MAJCOMs determine survey requirements of subordinate units based on criticality of mission. There are two types of surveys, formal and command (in-house).

5.3.5.1. Formal Survey. A formal survey concentrates on activities that cross command lines. It requires a survey team composed of members from inside and outside the command.

5.3.5.2. Command Survey. A command survey concentrates on activities within the particular command or unit. It is performed using only command (in-house) personnel. This is the more common of the two survey methods and the one most Air Force units will conduct. The command survey can be conducted throughout all organizational levels within the Air Force, down to the squadron level.

5.3.5.3. Survey Procedures. Each survey is unique due to the nature of the information requiring control, the adversary collection capability and the environment of the activity to be surveyed. **Attachment 3** outlines specific survey procedures.

Table 5.1. OPSEC Assessment Types

Assessment Type	Purpose	Methodology	Frequency	Request Procedures	Reporting
Program Self-Assessment	-Program Health -Policy Compliance -Shortfalls	Self-Assessment by unit OPSEC PM/ Coordinator	Annual	N/A	OPSEC PM/ Coordinator reports to Unit CC and Up Channel to HHQ PM
Web Risk Assessment	OPSEC review of unit website	Website reviewed by 67 IOW as part of TMAP	Biennial	Unit CC requests through HHQ PM	Report to Unit CC
TMAP	ID vulnerabilities	Collect and analyze communications	Biennial	Unit CC requests through HHQ PM	Report to Unit CC
SAV	- Policy Compliance - Shortfalls - Provide Guidance	Wing OPSEC PMs assess subordinate units (if collocated)	Annual	N/A	Report to subordinate Unit CC and OPSEC PM or Coordinator
OPSEC Survey	Assess unit OPSEC practice and procedures	Team analyzes documentation and interview personnel for: - IO Threat - Critical Information - Operational Procedures - Potential Indicators & Vulnerabilities	As required	Command Survey: Done in-house Formal Survey: Unit CC requests through MAJCOM OPSEC PM	Out-brief and report to Unit CC
MDVA	Assess application of influence operations	IO Red Team simulates IO threats to identify vulnerabilities, operational impacts, & exercise threat response procedures	Every 3 years for installation with critical mission or subject to IO threats	Installation CC requests through MAJCOM OPSEC PM	Out-brief & report to installation CC

5.3.6. Multi-Discipline Vulnerability Assessments (MDVA). MDVAs are performed to assess an installation's application of Influence Operations and security processes. MDVAs simulate various IO threats to identify an installation or organization's vulnerabilities (OPSEC, network, physical security, etc.), operational impacts if those vulnerabilities are exploited and exercise response procedures to the simulated threat. MDVAs directly support AFPD 10-7, *Information Operations*. These assessments are performed by a combined IO Red Team of AFIWC information warfare aggressors, Office of Special Investigations (OSI) Human Intelligence (HUMINT) Vulnerability Assessment Team and a TMAP team. MDVAs are not synonymous with Joint Staff Integrated Vulnerability Assessments or Air Force Vulnerability Assessments. However, installations may use MDVAs to satisfy the DODI 2000.16 and AFI 10-245 Red Teaming requirement. The IO Red Team conducts the MDVA in an adversarial role with the specific mission focus provided by the installation commander. An MDVA should be conducted every three years at installations with critical missions or significant IO threats. MDVA results are detailed in a formal report to the requesting commander. An MDVA should not be used to initiate an OPSEC program or used to prepare for an inspection. Commanders can request a MDVA by contacting their Wing, MAJCOM, ANG, FOA or DRU. An annual call-out message is normally released in the Spring. Out-of-cycle requests are submitted through MAJCOM, ANG, FOA or DRU PMs to ACC/DOZ. MDVAs may be augmented by MAJCOM force protection specialists.

5.3.7. Inspector General (IG) Evaluations. OPSEC programs will be evaluated during operational readiness inspections and unit compliance inspections. Additional guidance is provided in AFI 90-201, *Inspector General Activities*. MAJCOM, ANG, FOA and DRU PMs will coordinate with their respective IG team to ensure OPSEC evaluation criteria are current and IAW unique guidance from the MAJCOM, ANG, FOA, or DRU commander.

5.4. Assessment Reporting. Detailed results of OPSEC assessments are provided only to the requesting commander. However, assessment teams must share sanitized lessons learned, on a non-attribution basis, within the Air Force OPSEC community via the IO Threat Analysis Center. The IO Threat Analysis Center will provide detailed analysis and disseminate warranted information to OPSEC PMs and Coordinators worldwide.

NORMAN R. SEIP, Maj Gen, USAF
Acting DCS Air & Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

National Security Decision Directive (NSDD) No. 298, National Operations Security Program, 22 January 1998

DODD 5205.2, DOD Operations Security (OPSEC) Program, 29 November 1999

DOD Directive 5100.20, The National Security Agency and the Central Security Service, 23 December 1971

DOD Directive 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection, 10 September 1997

Joint Pub 3-54, Joint Doctrine for Operations Security, January 24, 1997

CJCSI 3213.01B, Joint Operations Security, 17 December 2003

DODD 3600.1, Information Operations, dated December 9, 1996

DOD 5230.9, Clearance of DOD Information for Public Release, April 9, 1996

DODD 8500.1, Information Assurance, October 24, 2002

DODD 5200.1-R, DOD Information Security Program, December 13, 1996

AFDD 2-5, Information Operations, 3 February 2005

AFPD 10-20, Air Force Defensive Counterinformation Operations, 1 October 1998

AFMAN 37-123, (will convert to 33-363) *Management of Records*

AFI 33-129, Web Management and Internet Use, 3 February 2005

AFI 33-219, Telecommunications Monitoring and Assessment Program (TMAP), 23 May 2002

AFPD 90-2, Inspector General -- The Inspection System, 1 September 1999

Abbreviations and Acronyms

AFOSI—Air Force Office of Special Investigations

CJCS—Chairman of the Joint Chiefs of Staff

CJCSI—Chairman Joint Chief of Staff Instruction

CIL—Critical Information List

DOD—Department of Defense

DODD—Department of Defense Directive

EW—Electronic Warfare

FOIA—Freedom of Information Act

HUMINT—Human Intelligence

IO—Information Operation

IOSS—Interagency OPSEC Support Staff

IW—Information Warfare

JCS—Joints Chiefs of Staff

JP—Joint Publication

MDVA—Multi-disciplined Vulnerability Assessment

NSC—National Security Council

NSDD—298 National Security Decision Directive 298

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

OPSEC—Operations Security

PM—Program Manager

PSYOP—Psychological Operations

RDS—Records Disposition Schedule

SAP—Special Access Program

Terms

Acceptable Level of Risk—An authority's determination of the level of potential harm to an operation, program, or activity due to the loss of information that the authority is willing to accept.

Acquisition Program—A directed and funded effort that is designed to provide a new, improved, or continuing weapons system or automated information system capability in response to a validated operational need.

Adversary—An individual, group, organization or government that must be denied critical information. Synonymous with competitor/enemy.

Adversary Collection Methodology—Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof.

Analysis—The process by which information is examined in order to identify significant facts and/or derive conclusions.

Assessment—To evaluate the worth, significance, or status of something; especially to give an expert judgment of the value or merit of something.

Countermeasure—Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

Counterintelligence (CI)—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Critical Information—Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Critical Information List (CIL)—Those areas, activities, functions, or other matters that a facility/organization considers most important to keep from adversaries.

Critical Program Information (CPI)—Information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.

Freedom of Information Act (FOIA)—A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Information Operations (IO)—Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Multi-disciplined Vulnerability Assessment (MDVA)—A systematic analytical process performed to assess an installation's application of influence operations and security processes to determine specific vulnerabilities. MDVAs simulate various IO threats to identify an installation or organization's vulnerabilities (OPSEC, network, physical security, etc.), operational impacts if those vulnerabilities are exploited and exercise response procedures to the simulated threat. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, terrorism, sabotage or espionage.

Observables—Any actions that reveal indicators which are exploitable by adversaries.

Operations Security (OPSEC)—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC Assessment—A thorough evaluation of the effectiveness of a customer's implementation of OPSEC methodology, resources, and tools. Assessments (a) are used to evaluate the effectiveness of the customer's corporate level OPSEC program and (b) can be used at the program level to determine whether or not a program is a viable candidate for an OPSEC survey.

OPSEC Coordinator—Below the wing and wing equivalent level. Acts as an interface to direct and manage all relevant OPSEC matters. Reports to OPSEC Program Manager

OPSEC Program Manager—At the wing and wing equivalent and above level. Focal point for OPSEC related matters and ensures OPSEC requirements are in compliance as directed from Higher Headquarters. Reviews operations plans to ensure a statement of OPSEC considerations and appropriate guidance regarding Critical Information are included.

Operations Security Indicator—Any detectable activity and/or information that, when looked at by itself or in conjunction with something else, allows an adversary to obtain critical or sensitive information.

Operations Security Process—An analytical process that involves five components: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures (NSC 1988).

Operations Security Program—An OPSEC program is the vehicle by which the principles and practices of OPSEC are employed within an organization.

Operations Security Survey—The application of OPSEC methodology at the program level. It is a detailed analysis of all activities associated with a specific operation, project or program in order to determine what exploitable evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries.

Operations Security Working Group (OWG)—A (normally formally) designated body representing a broad range of line and staff activities within an organization that provides OPSEC advice and support to leadership and all elements of the organization.

Risk—A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

Risk Analysis—A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.

Risk Assessment—An OPSEC process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity.

Sensitive Information—Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (NSTISSI 1997)..

Special Access Program—A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level (NSC EO 1995).

Threat—The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations.

Threat Analysis—An OPSEC process, which examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

Threat Assessment—An evaluation of the intelligence collection threat to a program activity, system, or operation.

Vulnerability—A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to prove a basis for effective adversary decision making.

Vulnerability Analysis—In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. See also information operations; information system; security; vulnerability.

Vulnerability Assessment—An evaluation (assessment) to determine the vulnerability of an installation’s application of influence operations and security processes to determine specific vulnerabilities. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, terrorism, sabotage or espionage.

Attachment 2

THE OPSEC PROCESS

A2.1. General. OPSEC is accomplished through the use of a five-step process. The five steps are: 1) identification of critical information; 2) threat analysis; 3) vulnerability analysis; 4) risk assessment and 5) application of appropriate measures. Although these steps are normally applied in a sequential manner during deliberate or crisis action planning, dynamic situations may require any step to be revisited at any time. The OPSEC process is cyclical in nature. This attachment briefly overviews the OPSEC process, for more detailed information see AF TTP 3-1 Vol. 36 (SIPRNet:**http://iwtactics.afiwc.aia.Kelly.af.smil.mil/home**).

A2.2. Step One: Identification of Critical Information. Critical information is information about friendly (U. S., allied and/or coalition) activities, intentions, capabilities or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, or cause loss of lives or damage to friendly resources. Critical information may also be derived from seemingly unrelated elements of information known as indicators. The product of the first step in the OPSEC process is a CIL.

A2.2.1. Critical information is best identified by the individuals responsible for the planning and execution of the unit's mission. An OWG can most effectively accomplish this task. Once a CIL is developed, commanders must approve the list and then ensure their critical information is protected and/or controlled.

A2.2.2. Critical information should be identified at the earliest possible time, preferably during the planning phases of an operation. Subordinate and supporting organizations should be apprised of operational information determined to be critical so they too can protect this information as well as any associated indicators.

A2.2.3. Revise your CIL as required reflecting changing mission/operational requirements. While categories of critical information are fairly stable, specific items of information are normally only critical for a prescribed period of time. The need to control or protect specific items of information changes as the mission/operation progresses or the threat changes.

A2.2.4. Critical information can be unclassified or classified. Unclassified critical information can be labeled Sensitive But Unclassified (SBU) or For Official Use Only (FOUO). In most cases, unclassified information identified as critical is described as Sensitive but Unclassified.

A2.3. Step Two: Threat Assessment. Current threat information is extremely important in developing appropriate OPSEC measures. The threat assessment includes identifying potential adversaries and their associated capabilities, limitations and intentions to collect, analyze and use critical information and OPSEC indicators.

A2.3.1. The AFOSI produces CI studies. AFOSI analyzes multi-disciplinary intelligence to evaluate threats from foreign intelligence services. This helps to protect both Air Force and DOD personnel and resources. AFOSI detachments produce local counterintelligence and criminal threat assessments on an annual basis. These assessments provide valuable input for OPSEC program decisions. AFOSI detachments may also produce focused counterintelligence studies when requested. Threat data can also be obtained through various other sources to include the Information Operations Threat Analysis Center and local intelligence units upon request.

A2.4. Step Three: Vulnerability Analysis. An OPSEC vulnerability exists when the adversary is capable of collecting an OPSEC indicator, analyzing it and then acting quickly enough to affect their decision making process. Vulnerabilities are weaknesses that reveal critical information through collected and analyzed indicators.

A2.4.1. OPSEC indicators are those friendly actions and information that adversary intelligence efforts can potentially detect or obtain and then interpret to derive friendly critical information. Indicators may be classified or unclassified.

A2.5. Step Four: Risk Assessment. OPSEC program managers and coordinators, in concert with other planners and with the assistance of intelligence and counterintelligence organizations, will provide risk assessments and recommend actions to senior decision-makers and commanders. Commanders must then decide whether or not to employ recommended OPSEC measures.

A2.5.1. Risk assessment involves an estimate of an adversary's capability to exploit a vulnerability, the potential effects such exploitation will have on operations and a cost-benefit analysis of possible methods to control the availability of critical information to the adversary.

A2.5.2. The guiding principles of ORM, managing all dimensions of risk to maximize mission effectiveness and sustain readiness, must be applied to OPSEC. Applying these principles will ensure that unnecessary OPSEC risks are avoided and that OPSEC risks are accepted when the cost of mitigation outweighs the benefit. Costs and benefits are likely to be operational versus monetary.

A2.6. Step Five: OPSEC Measures. Recommended OPSEC measures are designed to preserve military capabilities by preventing adversarial exploitation of critical information. OPSEC measures are employed to mitigate or exploit vulnerabilities that point to or divulge critical information. They help control critical information by managing the raw data and enhance friendly capabilities by increasing the potential for surprise and effectiveness of friendly military forces and weapons systems.

A2.6.1. OPSEC measures consist of a combination of IO capabilities that counter an adversary's ability to "gain" and "exploit" friendly information. These measures must be implemented as part of an overall IO effort to influence the adversary's perceptions and situational awareness.

A2.6.2. OPSEC measures fall under three general categories: 1) Preventing the adversary from detecting critical information and indicators; 2) providing alternative deceptive interpretations of critical information and/or indicators; and 3) attacking the adversary's collection system (JP 3-54, Appendix D).

A2.6.2.1. OPSEC measures prevent the adversary from detecting critical information and indicators. The objective is to eliminate or disrupt effective adversary information gathering of indicators or the vulnerability of actions to exploitation by adversary intelligence systems.

A2.6.2.2. OPSEC measures providing alternative interpretations. Sometimes it may not be cost-effective to control actions that reveal critical information or become the source of an OPSEC indicator. In these circumstances, measures attempt to influence and affect the adversary's ability to properly interpret the information.

A2.6.2.3. The third category of OPSEC measures is to use IO capabilities or kinetic operations to attack an adversary's intelligence collection system and thus eliminate or reduce their ability to obtain critical information. Two examples of this are: electronic attack against technical collection platforms and physical destruction of intelligence fusion and analysis centers.

A2.6.3. All OPSEC measures must be synchronized with other components of IO. These measures must be implemented as part of an overall IO effort to influence the adversary's perceptions and situational awareness. Care must be taken so that OPSEC measures do not become unacceptable indicators themselves.

Attachment 3

SAMPLE OPSEC SELF-ASSESSMENT CHECKLIST

NOTE: This is only an example to be used to develop your own inspection checklists based on your particular organizational level and/or OPSEC requirements IAW this instruction.

Administrative Requirements

1. Has the commander (all levels):
   a. Appointed an OPSEC Program Manager (PM) or coordinator and alternate in writing? (Para 2.1.2.1, **3.1.1.**, **3.2.** and **3.3.**)
   b. Ensured the OPSEC PM or coordinator has a security clearance appropriate to the mission and function of the organization, but not lower than Secret? (Para **3.2.** and **3.3.**)
2. OPSEC PM and/or Coordinator:
   a. Does the appointee reside in the operations or plans element of the organization or report directly to the organization's commander? (Para **3.1.2.**)
   b. Has his/her identity been forwarded to the higher headquarters (HHQ) OPSEC PM? (Para **3.2.** and **3.3.**)
   c. Is the OPSEC PM/coordinator aware of their responsibilities? (Para **3.2.1.** and **3.3.1.**)

OPSEC Execution Requirements

1. Has the commander (all levels):
   a. Developed an OPSEC program IAW HHQ policy and guidance? (Para 2.1.2.2)
   b. Ensured his/her organization has integrated OPSEC within day-to-day operations? (Para **3.1.1.**)
   c. Made OPSEC risk management decisions? (Para 2.1.2.2 and **3.1.1.**)
   d. Directed the overall implementation of OPSEC measures? (Para 2.1.2.2 and **3.1.1.**)
   e. Ensured OPSEC is integrated with other IO activities and efforts? (Para 2.1.2.2, **3.1.3.1.** and **3.1.4.**)
2. Has the OPSEC PM (wing-level and above):
   a. Developed, coordinated and managed the OPSEC program? (Para 2.1.2 and **3.2.1.1.**)
   b. Overseen development of commander's policy and creation of CILs (Para 2.1.2.5, **3.2.1.4.** and **3.2.1.4.**)?
   c. Developed procedures to ensure subordinate units are controlling critical information and indicators (Para 2.1.2.6 2.1.2.16 and **3.2.1.5.**)?
   d. Ensured subordinate units plan, exercise and implement OPSEC measures as appropriate? (Para 2.1.2.7 – command-level only)

e. Developed, coordinated and implemented an OPSEC plan? (Para **3.1.3.3.** and **3.2.1.1.**)

f. Incorporated OPSEC into organizational plans, exercises, activities and command-to-command agreements? (Para **3.1.3.**, **3.1.3.3.** and **3.2.1.2.**)

g. Incorporated OPSEC lessons learned from unit operations and exercises as well as other operations and exercises into the planning process and forward lessons learned to appropriate depositories? (Para **3.2.1.3.**)

h. Ensured all applicable contracts, Statements of Work (SOW), Requests for Proposals (RFP) and similar documentation contained specific statements or requirements that address security criteria for protecting OPSEC critical information and OPSEC indicators? (Para **3.1.3.** and **3.2.1.15.**)

i. Ensured OPSEC considerations are integrated into the acquisition cycle? (Para 2.1.2.8 and **3.2.1.15.**)

j. Developed and cultivated the intelligence and counterintelligence relationships necessary to support their OPSEC program? (Para 2.1.2.9)

k. Ensured OPSEC considerations are included in annual unclassified web page reviews and in the approval process for posting new data to the web? (Para 2.1.2.10, 2.1.2.11, **3.2.1.6.**, **3.2.1.7.** and AFI 33-129)

l. Ensured OPSEC considerations are included in PA's review and approval process for the publishing and/or releasing of information to or that may be viewed by the public? (Para 2.1.2.11 and **3.2.1.7.**)

m. Coordinated and facilitated OPSEC assessments IAW **Chapter 5**, AFI 10-701? (Para **3.2.1.13.**)

n. Completed an annual self-assessment of their program and each subordinate organization? (Para 2.1.2.14, wing-level)

o. Coordinated their OPSEC program with host or tenant unit OPSEC Managers and/or Coordinators? (Para **3.2.**)

p. Ensured OPSEC is integrated with other Information Operations (IO) activities and efforts? (Para **3.2.1.9.**)

q. Formed and chaired the OPSEC Working Group (normally wing-level) consisting of appropriate IO and security disciplines and applicable supporting organizations? (Para **3.2.1.12.**)

r. Conducted Staff Assistance Visits (SAVs) to all subordinate units as required? (**3.2.1.16.**)

s. Ensured all subordinate units are controlling critical information and indicators as required? (Para 2.1.2.16, command-level)

t. Ensured all subordinate units plan, exercise and implement OPSEC measures as appropriate? (Para 2.1.2.17, command-level)

u. Ensured OPSEC considerations are included in Initial Capabilities Documents, Capability Development Documents and inputs to the combatant commanders' Integrated Priority Lists as appropriate? (Para 2.1.2.18, command-level)

v. Ensured OPSEC reviews consider the proliferation of internet/web-based bulletin boards and logs (blogs)? (Para **3.2.1.8.**)

w. Serve as the focal point for TMAP (AFI 33-219)? (Para **3.2.1.17.**)

x. Established and chair a wing- (or wing equivalent) level OPSEC working group (OWG)? (Para 3-5)

y. Requested, for the commander, an MDVA if one has not been conducted in three years? (Para **5.3.6.**)

3. Has the OPSEC Coordinator (below wing-level):

a. Implemented and executed OPSEC utilizing commander and OPSEC PM policy and guidance? (Para **3.3.1.1.**)

b. Incorporated OPSEC into organizational plans, exercises and activities? (Para **3.1.3.** and **3.3.1.2.**)

c. Submitted lessons learned from operations and exercises to respective HHQ OPSEC PM.? (Para **3.3.1.3.**)

d. Overseen development and implementation of commander's OPSEC policy and CIL? (Para **3.3.1.4.**)

e. Developed procedures to ensure critical information is controlled and indicators identified? (Para **3.3.1.5.**)

f. Conducted OPSEC reviews on unit web pages prior to information being placed on the web page? (Para **3.3.1.6.** and **3.3.1.7.**)

g. Ensured OPSEC reviews are conducted on information to be published or released to or that may be viewed by the public? (Para 2.1.2.11 and **3.3.1.7.**)

h. Conducted an annual OPSEC survey? (Para **3.3.1.9.**)

i. Participated in OPSEC Working Groups as required? (Para **3.3.** and **3.3.1.10.**)

j. Coordinated and forwarded OPSEC assessment requirements to HHQ, IAW **Chapter 5**, AFI 10-701? (Para **3.3.1.11.**)

k. Utilized assessment results to correct discovered vulnerabilities and aid organization OPSEC awareness efforts? (Para **3.3.1.12.**)

l. Integrated OPSEC into all acquisition programs and contractor support documents? i.e., SOW, RFP and similar documentation will contain specific statements or requirements that address security criteria for protecting OPSEC critical information and OPSEC indicators. (Para **3.1.3.** and **3.3.1.14.**)

m. Coordinated their OPSEC program (tenant units only) with host unit OPSEC PMs and/or Coordinators? (Para **3.3.**)

n. Coordinated with appropriate organizations and wing/wing-equivalent senior leadership to resolve/mitigate Web Risk Assessment, TMAP, MDVA and other OPSEC assessment findings as required? (Para **3.3.1.15.**)

o. Serve as the unit focal point for TMAP (AFI 33-219). (Para 3.3.1.16)

Training Requirements

1. Has the OPSEC PM (wing-level and above):
   a. Attended OPSEC PM training within 90 days of their appointment or are scheduled for the next available Air Force OPSEC PM course? (Para **4.1.2.1.**)
   b. Ensured OPSEC training for coordinators below wing level is scheduled within 90 days of appointment, or by the next available class? (**4.1.2.1.**)
   c. Ensured all OPSEC Planners and personnel performing OPSEC surveys and IG inspections are provided OPSEC training? (Para **4.1.2.1.**)
   d. Maintained a general awareness of current OPSEC related events and sought continuation training at every opportunity? (Para **4.1.2.1.**)
   e. Ensured mission-oriented OPSEC education and awareness training was provided to all personnel on an annual basis? (Para 2.1.2.12 and **3.2.1.10.**)
2. Has the OPSEC coordinator (below wing-level):
   a. Been scheduled for OPSEC training within 90 days of the assignment as an OPSEC Coordinator? (Para **4.1.2.2.**)
   b. Provided management and oversight of initial OPSEC training upon arrival of newly assigned personnel (military, civilian and contractors) and recurring training annually thereafter? (Para 2.1.2.12, **3.3.1.**.8and **4.1.1.**)
   c. Ensured OPSEC training for newcomers and annual recurring training contain, as a minimum the unit's critical information, threats to the unit and applicable OPSEC measures to be used? (Para **4.1.1.2.**)
   d. Tracked and documented training for all military, civilian and contractor personnel (Para **4.1.1.** and **4.1.1.3.**)?

OPSEC Assessment Requirements

1. Has the OPSEC PM (command-level):
   a. Coordinated closely with subordinate organization to determine assessment requirements? (Para **5.2.**)
2. Has the OPSEC PM (wing-level):
   a. Conducted annual SAVs of their subordinate units? (Para **5.3.4.**)
3. Has the OPSEC PM or Coordinator:
   a. Conducted an annual self-assessment? (Para 2.1.2.14, **3.1.5.** and **5.3.1.**)
   b. Had a telecommunications monitor conducted as part of a survey, an MDVA, or a stand-alone assessment at least biennially? (Para **5.3.3.**)
   c. Conducted or had an outside agency conduct a survey? (Para **5.3.5.**)

d. Ensured OPSEC reviews considered the proliferation of internet/web-based bulletin boards and logs (blogs) and evaluate the risk presented by web content in annual OPSEC assessments. (Para **3.2.1.8.**)

OPSEC Reporting Requirements

1. Has the OPSEC PM (wing-level and above):

   a. Developed and submitted to HHQ an annual budget requirement for inclusion into command and HQ USAF POM process? (Para 2.1.2.3 and **3.2.1.11.**)

   b. Forwarded their self-assessment findings containing:

      (1) training metrics for all subordinate units, (Para **4.1.1.3.**, 2.1.2.14),

      (2) number of vulnerability reports forwarded to the IO Threat Analysis Center, (Para 2.1.2.14 and **3.2.1.14.**)

      (3) number and type of survey/assessment received by subordinate units (command survey, TMAP, MDVA, Web Risk Assessments, etc.), (Para 2.1.2.14 and **3.2.1.13.**) and

      (4) any other information deemed of OPSEC importance to their HHQ OPSEC PM NLT 30 September and of each year? (Para 2.1.2.14, **3.2.1.11.** and **3.3.1.11.**)

   c. Ensured OPSEC vulnerability reports are forwarded to HQ AIA's IO Threat Analysis Center in a timely manner? (Para 2.1.2.15, **2.2.1.** and **3.2.1.14.**)

2. Has the OPSEC Coordinator (below wing-level):

   a. Forwarded their self-assessment findings containing:

      (1) training metrics for all personnel, (Para **4.1.1.** and **4.1.1.3.**),

      (2) number of vulnerability reports forwarded to the IO Threat Analysis Center, (Para 2.1.2.14 and **3.2.1.14.**)

      (3) number and type of survey/assessment conducted (command survey, TMAP, MDVA, Web Risk Assessments, etc.), (Para 2.1.2.14 and **3.3.1.11.**) and

      (4) any other information deemed of OPSEC importance to their HHQ OPSEC PM NLT 15 September of each year? (Para **3.3.1.11.**)

   b. Submitted OPSEC vulnerability reports for forwarding to HQ AIA's IO Threat Analysis Center in a timely manner? (Para **3.3.1.13.**)

Attachment 4

SURVEY EXECUTION

1. General

a. The OPSEC survey is a systematic process to examine the actual practices and procedures employed by an activity or operation to achieve its goals. The methodology consists of using a team of experts to look at an activity through the eyes of an adversary to determine if critical information may be inadvertently disclosed through the performance of normal organizational functions. The primary purpose is to evaluate and improve organizational effectiveness and to control the vulnerabilities of friendly actions or information.

b. The survey will determine if the critical information identified during the OPSEC planning process is being protected or controlled. A survey cannot be conducted until after an organization has at least identified its critical information. Without a basis of identified critical information, there can be no specific determination that actual OPSEC vulnerabilities exist.

2. Uniqueness

a. Each OPSEC survey is unique. Surveys differ in the nature of the information requiring protection or control, the adversary collection capability and the environment of the activity to be surveyed.

b. In times of crisis or conflict, a survey's emphasis must be on identifying operational indicators that signal friendly intentions, capabilities and/or limitations and that will permit the adversary to counter friendly operations or reduce their effectiveness.

c. In peacetime, surveys generally seek to correct weaknesses that disclose information useful to potential adversaries. Many activities, such as mobility exercises, cradle-to-grave acquisition processes and day-to-day operations/training are of strategic interest to potential adversaries as they provide insight into friendly readiness, plans and capabilities.

3. OPSEC Surveys Vs. Security Inspections

a. OPSEC surveys are different from security evaluations or inspections. A survey attempts to produce an adversary's view of the operation or activity being surveyed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

b. Surveys are planned, coordinated or conducted by the organization responsible for the operation or activity that is to be surveyed. Inspections may be conducted without warning by outside organizations.

c. OPSEC surveys are not a check on the effectiveness of an organization’s security programs or its adherence to security directives. Instead, survey teams will assess how current security measures positively or negatively affect OPSEC.

d. Surveys are not punitive by nature and no grades or evaluations are awarded as a result of them. Surveys are not designed to inspect individuals but to evaluate practices and procedures used to accomplish the mission. Unless this non-punitive objective is made clear, team members will inevitably appear as inspectors, which may hamper cooperation and assistance from the surveyed organizations.

4. Types of Surveys. There are two basic kinds of OPSEC surveys: formal and command.

a. Both types of surveys follow the same basic sequence and procedures that are established in this attachment.

b. A formal survey concentrates on activities that cross organizational lines. It requires a survey team composed of members from inside and outside the command.

c. A command survey concentrates on activities within the particular command/unit. It is performed using only command/unit (in-house) personnel. This is the most common survey for Air Force units.

5. Survey Execution.

Careful prior planning, thorough data collection and thoughtful analysis of the results are the key phases of an effective survey. There are three phases to a survey, the Planning Phase, the Field Survey Phase and the Analysis and Reporting Phase. The following text describes each phase.

OPSEC SURVEY PLANNING PHASE

Preparations for an OPSEC survey must begin well in advance of the field survey phase. The required lead-time will depend on the nature and complexity of the operation and activities to be surveyed (contingency operation, peacetime operational activity, or other type of operation). Sufficient time must be allotted in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions and for the careful preparation of functional outlines. The following actions normally make up the planning phase.

a. Determine the Scope of the Survey.
The scope of the survey should be defined at the start of the planning phase and be limited to manageable proportions. For example, an internal command survey conducted by a squadron would require less time and coordination than a formal survey and would be limited to actions within the resource and manpower limitations of the squadron. Geography, time, units to be observed, funding and other practical matters will also impose limitations.

b. Select Team Members.
Regardless of the survey's focus, the team should contain multidiscipline expertise. Survey team members should be selected for their analytical, observational and problem-solving abilities.

Since surveys are normally oriented to operations, the senior member should be selected from the operations (or equivalent) staff of the commander responsible or conducting the survey.

Typical team members would represent the functional areas of intelligence, security, counterintelligence, communications, logistics, plans and personnel. When appropriate, specialists from other functional areas, such as transportation and public affairs, will participate.

When TMAP is planned as part of the survey, the monitoring team's mission supervisor or senior analyst should be designated as a member of the OPSEC survey team. Team members must be brought together early in the planning phase to ensure timely, thorough accomplishment of the tasks outlined below.

c. Become Familiar with Survey Procedures.

When possible, designate team members with survey experience. Otherwise, train team members on survey procedures.

d. Determine the Adversary Intelligence Threat.

The adversary threat to the organization to be surveyed must be evaluated accurately, carefully and realistically. An all-source threat assessment should comprehensively address the adversary intelligence capability, taking into account not only the adversary's collection capabilities but also the adversary's ability to exploit the collection results in a timely manner. Survey team members can obtain adversary threat information from multiple sources including the local AFOSI detachment, HQ AFOSI's Local Threat Assessment, Defense Intelligence Agency, AFIWC and the Air Intelligence Agency.

e. Understand the (Target) Organization.

A thorough understanding of the organization to be surveyed is crucial to ensuring the success of subsequent phases of the survey. Team members should become familiar with the mission statement/description, OPLANS, OPORDS, CONOP, standard operating procedures, or other directives bearing on the surveyed organization.

f. Develop a Functional Outline.

A basic OPSEC survey technique involves the construction of a chronology of events that are expected to occur in the surveyed operation or activity. Events are assembled sequentially, thus creating a timeline that describes in detail the activities or plans of an operation or activity.

Chronologies should first be constructed for each separate functional area, such as operations, communications, logistics, or personnel. This functional approach aids the team members in defining their separate areas of inquiry during the field or data collection phase of the survey. Later, the functional outlines can be correlated with each other to build an integrated chronology of the entire operation or activity.

During the initial review of operation plans, orders and procedures, individual team members can begin to develop functionally oriented outlines for their areas of interest. Initially, the outlines will be skeletal projections, in a narrative, table, or graph format, of what is expected to occur in the chronology for a particular functional area.

Such projections can serve as planning aids for the subsequent field survey phase. For example, units and facilities associated with each of the events can be identified and geographically grouped to aid in planning the travel itinerary of team members during the field survey. Collectively, the initial functional outlines provide a basis for planning the field survey phase and constitute a basis for observation and interviews.

During the field survey phase, team members will acquire additional information through observation, interviews and other data-collection techniques, enabling further development and refinement of the functional outlines.

Collectively, the outlines project a time-phased picture of the events associated with the planning, preparation, execution and conclusion of the operation or activity. The outlines also provide an analytic basis for identifying events and activities that are vulnerable to adversary exploitation.

After the chronology is assembled, vulnerabilities can be identified in light of the known or projected threat.

g. Determine Preliminary Friendly Vulnerabilities.

After the adversary intelligence threats are determined, a subjective evaluation can be made of the potential friendly vulnerabilities. A vulnerability (e. g., a detectable, exploitable event) may or may not carry a security classification at the time of its identification, but such preliminary vulnerabilities must be protected from disclosure by administrative or security controls.

h. Announce the Survey.

After team members are selected and are familiar with the organization to be surveyed, the organization conducting the survey should inform its subordinate and supporting organizations that a survey will be conducted so that preparations can be made to support the team during the field survey phase. The following information should be included:
(1) Survey purpose and scope.
(2) List of team members and their clearances.
(3) List of required briefings and orientations.
(4) Timeframe involved.
(5) Administrative support requirements.
(6) TMAP support requirements (if needed).

OPSEC FIELD SURVEY PHASE

As noted previously, data collection begins in the planning phase with a review of associated documentation. During the field survey phase, interviews with personnel directly involved in the operation, together with observations and document collection, are the primary means of data collection. The following actions are normally accomplished during the field survey phase.

a. Command Briefing on Operation to be Surveyed.
This briefing is presented to the OPSEC survey team by the command directing the forces or assets involved in the operation or activity being surveyed. The purpose of the briefing is to provide the survey team with an overview of the operation from the command's point of view. Team members should use this opportunity to clarify remaining questions about the information developed in the planning phase.

b. OPSEC Survey Team In-Brief.
The survey team chief presents this briefing to the commander and principal staff officers of the surveyed organization. The briefing may be either a formal presentation or an informal discussion. The objective is to inform the commander and the staff of how the survey will be conducted. The briefing should include a summary of the hostile threat and the vulnerability assessment developed during the planning phase. Results of previous OPSEC surveys of similar activities may be summarized. The commander should be given the opportunity to recommend specific focus areas for the survey team to concentrate on.

c. Data Collection and Functional Outline Refinement.

During the field survey phase, data is collected through observation of activities, document collection and personnel interviews. Data may also be acquired through concurrent data collection, such as TMAP.

Team members must be alert to differences between what they have read, what they have assumed to be the situation, what they have been told in the command briefing and what they observe and are told by personnel participating in the operation. Conflicting data is to be expected.

While observations can verify the occurrence, sequence and exact timing of events, much essential information must be gathered from interviews.

(1) Functional outlines should be reviewed before and after interviews to ensure that all pertinent points are covered. Specifics on how, when and where people accomplish their tasks and how these tasks relate to the planned and observed sequence of events, are recorded in order to document activities in a logical sequence.
(2) Team members should assure interviewees that all sources of information will be protected by a non-attribution policy.
(3) Interviews are best conducted by two team members.
(4) Facts to be recorded during or soon after the interview normally include:
(a) Identification and purpose of the interview.
(b) Description of the positions occupied by the persons being interviewed.

(c) Details of exactly what tasks the individuals perform and how, when and where they perform them with a view toward determining what information they receive, handle, or generate and what they do with it.
(d) Whether the individuals' actions reflect an awareness of a hostile intelligence collection threat.

Functional Outline Refinement.
As indicated earlier, each team member should have a basic functional outline to direct data collection efforts at the beginning of the field survey phase. The basic outline will be modified during this phase to reflect new information obtained by observation/interview and will ultimately become a profile of actual events.

Each team member should be familiar with the outlines used by the other members of the survey team and should be alert for information that might affect them. An interview in the communications area, for example, might disclose information that would result in a change to the outline being developed for operations; or an observation in one geographic location could affect an outline being followed up in another. Also, to permit follow-up elsewhere, all outlines should try to reflect the information generated and the flow at each location where data is collected.

As data is accumulated through observation and interviews, incorporation of such data into the basic functional outline changes the original list of projected events into a profile of actual events. The functional outline then becomes a chronological record of what actually was done, where, who did it and how and why it was done. The outline should also reflect an assessment of the vulnerability of each event to the known or suspected hostile intelligence threat.

Tentative observations will begin to emerge as data collection proceeds and information is reviewed and compared. The observations should be confirmed and fully documented as quickly as possible.

If an observation is considered to have serious mission impact, the organization's commander should be immediately notified in order to permit timely corrective actions.

Development of observations during the field survey phase ensures access to supporting data and precludes the need to reconstruct events after the team has departed. Following this procedure, the basic observations and supporting data of the final survey report will be well developed before the end of the field survey phase. Final development and production of the survey report can then proceed immediately upon the team's return to home station.

d. Team Employment.
The complexity, size and duration of the surveyed operation or activity will determine the general employment of the survey team. Tentative locations for data collection, developed during the planning phase, provide initial indications of how and where to employ the team.

It is rarely possible to accurately plan employment in detail before the field survey phase. A limited, short duration operation with few participating elements may permit concentrating the team in one or two locations. Larger and longer operations may require complete dispersal of the team, movement of the entire team from one location to another, or both, over a substantial period of time. The most reliable guideline for the team chief in determining how to employ the team is to reassemble it daily to assess progress, compare data and coordinate the direction of the survey.

The duration of the field survey phase is established during the planning phase and depends on how rapidly data is collected. The proximity of data collection locations to each other, number of such locations, transportation availability and degree of difficulty experienced in resolving conflicting data are some of the factors affecting duration of the field survey phase.

e. OPSEC Survey Team Out-Brief.
An out-brief should be presented to the commander before the team departs, regardless of previous reports or tentative observations. Like the in-brief, the out-brief can be an informal discussion with the commander or a formal briefing for the commander and the staff.

The tentative nature of survey observations should be emphasized. Even those that appear to be firm may be altered by the final data review as the survey report is prepared. Because preparation of the written report may take some time, the out-brief can serve as an interim basis for further consideration and possible action by the commander. The distribution of the final written report should be clearly stated during the out-brief. Normally, the report will be provided directly to the commander.

ANALYSIS AND REPORTING PHASE

During this phase, the OPSEC team correlates the data acquired by individual members with information from any other assessments conducted in conjunction with the survey.

a. Correlation of Data

Correlation of Functional Outlines. When the separate chronology outlines for each functional area are correlated, the chronology of events for the organization will emerge. Data from the field survey and analytic phases must not conflict with each other.

Functional Outlines. The purpose of constructing the functional outlines is to describe the time-phased unfolding of the operation or activity; to depict the manner in which separate commands, organizations and activities interact and perform their roles in the operation or activity; and to trace the flow of information from its origin to its ultimate recipients. It is important that the team members present the information in a manner that facilitates analysis. The net result of the correlation will portray the practices and procedures of the entire organization.

b. Identification of Vulnerabilities

The correlation and analysis of data helps the team refine the previously identified preliminary vulnerabilities or isolate new ones. The analysis is accomplished similarly to the way adversaries would process information through their intelligence systems.

Potentially observable indicators are identified as vulnerabilities. The key factors of a vulnerability are observable indicators and an intelligence collection threat to those indicators.

The degree of risk to the friendly mission depends on the adversary's ability to exploit these vulnerabilities and react to the situation in sufficient time to degrade the organization's mission.

c. OPSEC Survey Report

The OPSEC survey report is addressed to the commander of the surveyed organization. The report provides a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis and recommended OPSEC measures to eliminate or reduce the vulnerabilities. Although some vulnerabilities may be virtually impossible to eliminate or reduce, they should be included in the report to enable commanders to realistically assess their organization.

Each report should contain a threat statement. Its length and classification need only be adequate to substantiate the vulnerabilities (or actual sources of adversary information) described in the report. Portions of the threat that apply to a particular observation should be substantiated in the report. If the classification level of the threat statement impedes the desired distribution and handling, consider attaching the threat statement in a separate annex to the report.

Recommendations for corrective actions should also be included in the report. However, the team is not compelled to accompany each observation with a recommendation. In some situations, the team may not be qualified to devise the corrective action; in others, it may not have an appreciation of the limitations in resources and options of a particular command. Ultimately, commanders must assess the effect of possible adversary exploitation of vulnerabilities on the effectiveness of their operation or activity. They must then decide to implement corrective actions or accept the risk posed by the vulnerability.

Appendixes and annexes to OPSEC survey reports may be added to support the observations, conclusions and recommendations. Some examples include threat assessments, maps, diagrams and other illustrative materials.

The report may end with a conclusion or summary of the survey and its findings. The summary should not include judgments about compliance with standing security practices of the organizations. Such judgments are the purview of security disciplines.

Because they contain vulnerability information, OPSEC survey reports must be controlled from release to unauthorized persons or agencies. Affected portions of the report must be controlled in accordance with applicable security classification guides. For those portions of the report not controlled by security classification guides, administrative control of the release of survey report information must be considered. Likewise, the notes, interviews and raw data used to build a survey report must be subject to the same controls as the finished report.

The following pages contain information and documentation to be used during the entire survey process. This information is to be used as a guide and units are to limit the scope of their survey to available manpower and resources.

OPSEC Survey Planning Worksheet

Phase 1 refers to all preparations done prior to the team beginning the information-gathering phase of the survey, which includes threat research, preparatory interviews and preliminary documentation search.

Phase 2 refers to the period when the entire team comes together, conducts interviews, holds daily team meetings, completes the analysis and reports the results.

The completed worksheet may be provided to team members at the beginning of Phase 2 in lieu of a written survey plan. Attachments too lengthy to provide individual copies may be made available in a separate notebook.

1	Team Leader Name		
2	Program, activity or unit to be surveyed		
3	Dates		
4	Team expertise required	❑ OPSEC ❑ Counterintelligence (CI) ❑ Physical Security ❑ Intelligence ❑ Other: ❑ Other: ❑ Other:	❑ Computer Security ❑ Systems Management ❑ Communications ❑ Local Mission ❑ Other: ❑ Other: ❑ Other:
5	Request team members from internal sources Due:	❑ Operations ____________ ❑ Communications ____________ ❑ Logistics ____________ ❑ Intelligence ____________ ❑ Security ____________ ❑ Security ____________ ❑ Security ____________ ❑ Security ____________ ❑ Admin ____________ ❑ Other ____________ ❑ Other ____________ ❑ Other ____________ ❑ Other ____________ ❑ Other ____________	
6	Request team members from external sources Due:	❑ IOSS ❑ AFIWC ❑ Other:	❑ CI (AFOSI, NCIS,Army MI) ❑ TMAP monitoring ❑ Other:
7	Team member clearances POC: Due: ❑ Clearances received	Send clearances to:	
8	Augmentee/instructor funding POC: Due:		

9	Billeting required for any team members? ❏ Yes ❏ No POC: Due:	Name: Dates: Location:
		Name: Dates: Location:
		Name: Dates: Location:
		Name: Dates: Location:
		Name: Dates: Location:
10	Open Source Research Provide a summary of information found in open source as attachment 1. POC: Due:	Data Bases
		Key Words
11	Threat Report Request a threat analysis report and provide as attachment 2. POC: Due:	Address to:
		Address to:

		Address to:		
		Specific information to request:		
12	Local documents POC: Due:	❑ Phone books ❑ Welcome packets ❑ Circulars ❑ Critical Information list		❑ Operating Instructions ❑ Local newspaper ❑ Local newsletter(s) ❑ Other
13	Arrange working space for the team POC: Due:	Location: ____ Hours available: ____		
14	Arrange administrative support for the team POC: Due:	Name/Phone/Email:		
15	Schedule in brief POC: Due:	Date:	Time:	Location:
16	Schedule threat brief POC: Due:	Date:	Time:	Location:
17	Schedule mission brief POC: Due:	Date:	Time:	Location:
18	Schedule dry run out brief POC: Due:	Date:	Time:	Location:
19	Schedule out brief POC: Due:	Date:	Time:	Location:

20	Pre-survey interviews List team member responsible for each interview; team members should provide a summary of their interview to the team leader. Attach these summaries as attachment 3. Interview summaries are due:	❑ Commander or Director	
		❑ Survey activity director	
		❑ Communications manager	
		❑ Network manager	
		❑ Computer Security officer	
		❑ COMSEC officer	
		❑ Security manager	
		❑ Physical security support	
		❑ Other:	
		❑ Other:	
		❑ Other:	
		❑ Other:	
21	Initial interview list POC: Due:	Include a list of personnel who should be interviewed when Phase 2 starts as attachment 4; include contact information for each person.	
22	Team member list POC: Due:	The team leader should compile a complete list of team members with contact information. If possible, identify partners. You may want to match interview teams with functional areas, at least to get started. Include the list as attachment 5.	
23	Commander's Letter POC: Due:	During Phase 2, every team member should carry a letter from the commander (or designee) identifying the team members and their authority to conduct interviews. This letter, along with appropriate picture identification, should admit team members to work areas and provide adequate identification for interviews.	
24	Adversary Strategy POC: Due:	Prepare a preliminary adversary strategy based on the team leader's assessment of adversaries to be included in the survey analysis. See sample adversary strategy template below.	
25	Process Diagram POC: Due:	Prepare a preliminary process diagram for the primary survey topic based on pre-survey interviews above.	

OPSEC Survey Planning Worksheet Instructions. The team leader has oversight responsibility for the completion of this worksheet, but should enlist members of the team to be responsible for specific action items and assign a due date for each action.

Item 1. Self-explanatory.

Item 2. Enter the name of the project, activity or unit to be surveyed, such as Operation Fire Fly; or assign a designator to the survey, such as 61TAG–1" (organization name) (first survey) or "61TAG–0101" (organization name) (fiscal year) (first survey).

Item 3. Enter the dates of Phase 2.

Item 4. Identify those expertise areas you will need represented on your team, based on the commander's requirements and the subject to be surveyed. If you anticipate needing access to such expertise to answer questions, but don't anticipate needing that expertise from team members, make such a notation.

Item 5. Identify the names of individuals within your own organization you would like to have on the team and their assigned functional areas.

Item 6. Identify which organizations you will need to ask for augmentees.

Item 7. All team members including those from outside units will need to provide proof of a current security clearance. Indicate the address, the date those clearances need to be confirmed and check the box when this action is complete.

Item 8. If you are asking for help from organizations other than your own, provide financial assistance for augmentee or instructor travel. This space is for whatever notes you need to complete this action.

Item 9. Team members may need assistance with billeting depending on the travel requirements for the OPSEC survey to be conducted. Be sure this is discussed and addressed as part of the planning phase.

Item 10. You will need to do some open source research to prepare for your survey. List the databases and key words you want to use.

Item 11. You should request a written threat report, which will become part of your final report. You may want to request threat information from more than one source; the checklist allows room for three. Also indicate any specific information you have requested.

Item 12. Indicate which local documents you want to have on hand for the team.

Item 13. The team will need a work area where you can hold team meetings in private, where team members can sit to write up interviews and their observations for the report. A white board or flip chart and a bulletin board in the room are very helpful.

Item 14. Administrative support for the team can be very helpful. This individual may not be needed until the last three days prior to the out-brief, but someone who has access to the local networks and is a proficient typist can relieve some of the administrative burden from the team. Someone who is good with briefing preparation may also be useful.

Item 15. Schedule a formal in-brief with the commander or program director and anyone else he/she feels appropriate. The purpose of the in-brief is to introduce the team, outline your task and get any last minute instructions from the commander.

Item 16. Schedule a formal threat brief for the team (if this wasn't done earlier in planning). If this action is not required, just indicate "N/A."

Item 17. Schedule an organizational mission brief for the survey team. Most organizations have a standard briefing that outlines the mission; that's what you want to hear, even if you think you already know all the information. This is especially important when you have augmentees on your team. If nothing else, it allows the team to see what the organization is briefing to outsiders.

Item 18. Schedule a dry run out-brief for the afternoon of the day before your formal out-brief. All team members should have the date, time and location prior to starting interviews and should invite everyone interviewed to the dry run. All team members should attend and you should encourage attendance of those with responsibility for areas you will be including in your report. For instance, if you're briefing insufficient secure communications, be sure those responsible for providing those communications are at the dry run. The dry run has two purposes. First, it gives the team leader a chance to go through the out-brief once with all team members present to provide clarification on rough spots. Second, it gives you a chance to enlist the aid of those responsible for the areas where the team found problems rather than causing any hard feelings or alienation and gives you one last validation of what you will report.

Item 19. Schedule a formal out-brief with the commander or his representative. It is a good idea to encourage the commander to have all functional area managers attend. The purpose of the out-brief is to tell the leadership what your survey found and to set the tone for follow-up actions on the part of the organization. In the best situation, the commander will assign actions and suspense dates for every observation during the briefing.

Item 20. As a minimum, all individuals should be interviewed prior to the start of Phase 2. This will give the team an idea of what vulnerabilities already have been identified and if there have been any corrective actions taken. You may have others you think should be interviewed to that end and those individuals may be added at “other.”

Item 21. An organizational chart may assist you in compiling this list. You should include phone and email address and building/room number if available. This will assist you in assigning interviews and to ensure all appropriate staff have been interviewed.

Item 22. There should be a complete list of survey team members, along with their contact information. You should provide this to every member of the team and include in the final report.

Item 23. Prepare an authorization letter for the commander’s signature; identify the purpose of the survey, the team member names and identification information, their clearance and the commander’s authority for them to conduct interviews. Team members should always carry it in case they are challenged or someone they are interviewing hesitates to cooperate. However, team members should only produce the letter when asked.

Item 24. Prepare a preliminary adversary strategy based on the team leader’s assessment of adversaries to be included in the survey analysis. The adversary strategy identifies friendly objectives and possible strategies the adversary will use to defeat and/or mitigate friendly objectives or intentions.

Item 25. A process diagram must be prepared for the unit, mission, or operation being studied. The process diagram is simply a graphic representation of the processes performed by the studied organization and the means used to communicate with both internal and external organizations. The process diagram allows you to determine possible vulnerabilities.

Attachment 5

OPSEC INTERVIEW CHECKLIST

Interviewee's Name/Unit: ________________________________ Phone: __________________

Interviewer(s): ______________________________________ Date/Time: __________________

Section 1: Overview *Note: to interviewer: We want to know how well personnel understand OPSEC and their responsibilities.*					
Unless otherwise noted, use the following scale for Section 1: 1) Very poor 2) Poor 3) Average 4) Good 5) Outstanding	1	2	3	4	5
1. What is operations security (OPSEC)? *Note to interviewer. Note whether or not the person can give you a reasonable explanation of OPSEC in general. Rate answer using the 1 to 5 scale below* Criteria: 1 = No understanding. 2 = Confuses OPSEC with something else (i.e. COMSEC). 3 = Understands that OPSEC protects critical information 4 = Understands OPSEC principles, but may not use correct terminology. 5 = Fully understands the concepts of critical info, threat, vulnerability, risk and countermeasures.					
2. Are you aware of your section/unit's OPSEC program? GYes or G No *Note to interviewer. If the person answers No, go on to question* 3. *If the answer is yes, ask the following:* How would you rate the OPSEC Program in terms of its contribution to mission success? 1 = Poor; 3 = Good; 5 = Excellent Why:					
3. Does your section/unit have an OPSEC Coordinator? GYes or GNo *Note to interviewer: If the person answers no, go on to question 4. If the answer is yes ask the following.* How would you rate your section/unit in terms of getting you the information you need on OPSEC? Why?					
4. Have you received OPSEC training from this organization? GYes or GNo *Note to interviewer. If the person answers no, go on to section 2. If the answer is yes ask the following:* How would you rate the OPSEC training you have received? Why?					

Section 2: Individual Rating

For Section 2 use the following scale: 1) Not at all 2) Slightly 3) Moderately 4) Mostly 5) Completely	1	2	3	4	5
1. OPSEC relates to my duties.					
2. I understand OPSEC sufficiently enough to employ its use.					
3. OPSEC receives sufficient emphasis in my section/unit.					
4. OPSEC receives sufficient emphasis in the organization.					
5. OPSEC is critical to the organization's mission.					

Section 3: Intelligence Threat

Note to interviewer. We need to determine how well the population understands the intelligence threat to their unit's/section's mission(s).

1. Programs that protect our information assume someone is out to get it. Do you believe there is a threat to THIS ORGANIZATION? GYes or GNo

Note to interviewer. If the person answers yes, ask the following.

Who (or what) do you think is a threat to the mission? (List countries, agencies, organizations, etc.) Please rate each as High or Medium or Low.

2. In OPSEC, threats are derived from adversaries. How do you think an adversary would collect or gather information about your section/unit's mission?

Note to interviewer. You may need to provide examples to demonstrate what you're talking about depending on the experience level of the interviewee. (i.e., monitoring of radio communications, foreigners soliciting information from you or your family, SATCOM, IMINT, etc.)

Section 4: Critical information

Note to interviewer. The objective is to determine how well individuals understand critical information.

1. What information about your mission/duties would an adversary want or need to know to be able to degrade or deny the mission? (<u>use adversaries point of view</u>)

2. What information about your mission needs protection from your point of view?

3. When you are doing an exercise or an operation how does the information you need to protect change, or does it change?

Section 5: Information Processing (Computers)

Note to interviewer. We're looking for what systems are used to process information and whether or not those systems are encrypted or otherwise protected.

1. Do you use a computer at work? GYes or GNo
Note to interviewer. If No, go on to question 2. If yes:
What percentage of your time do you spend on a classified system?
On an unclassified system?

2. Do you use e-mail? GYes or GNo
Percentage classified ________ Percentage unclassified __________
Do you use e-mail at home? GYes or GNo
Do you ever get business email at your home? GYes or GNo

3. Describe what you use your computer for; i.e. data base access, word processing, presentations, accessing Internet, etc.
Note to interviewer: We're especially interested in the various connections to other commands and/or national networks. Not interested in content!

4. Do you publish information on the world wide web (the Internet)? GYes or GNo
Any other web or Intranet? GYes or GNo
Do you provide personal or work-related information using internet based bulletin (blogs) or websites? GYes or GNo
Note to interviewer. If necessary very briefly describe.

5. Do you get involved in publishing information of any kind on the web or internet? GYes or GNo
Explain:

Section 5: Information Processing (Computers) Continued

Note to interviewer. We're looking for what systems are used to process information and whether or not those systems are encrypted or otherwise protected.

6. What networks do you use in your job? (i.e.. data base, web pages, SIPRNET, INTELINK)

7. Do you have NATO/COALITION/ALLIED interface? GYes or GNo

8. Do you use a laptop computer? GYes or GNo
Note to interviewer. If no, go on to question 10.
Is it encryption protected and approved for classified processing? GYes GNo GUnknown
Is it government owned? GYes or GNo

9. Do you use any other personal communications equipment? GYes or GNo
If yes, describe: (Examples include pagers, palm pilots, GPS devices, etc.)
Note to interviewer. Do not include cell phones or radios in this answer.

Section 6: Telephones

1. What percentage of your phone calls each day are not secure?

2. Do you have ready access to a STU-III or STE? GYes or GNo
Note to interviewer. If No, go on to question 3. If Yes, ask the following:
Where is the phone located? (i.e., on your desk, in a common room, in another office)

Where is the crypto-ignition key (CIK) kept?

For CIK's kept in a safe, do you know the combination? GYes or GNo
How is the CIK controlled? (i.e., only taken out to use it or, loaded first thing, put away last, etc.)

3. Do you have ready access to any other secure phone? GYes or GNo

4. Please tell me some of the vulnerabilities of using a secure phone in an office where others are working in close proximity.
Note to interviewer. Don't give hints, but we're looking for 2 things: (1) an understanding that intelligence can be gleaned from discussions before and after going secure, (2) the possibility sensitive background conversations will be transmitted over the open line.

Section 7: Cell phones

1. Do you use a government owned cell phone? GYes or GNo
If Yes, what are the vulnerabilities associated with cell phones?
Note to interviewer. Should discuss eavesdropping on activation, geo locating and ease of interception.

2. Do you use a personal cell phone? GYes or GNo
If Yes, Do you use it for work? GYes or GNo
Briefly what do you use it for? (non-attribution)

3. What if any, are the rules for bringing cell phones into work areas?

Section 8: Radios
1. Do you use a radio regularly for official business? GYes or GNo *Note to interviewer. If No, go to question 2. If yes, ask the following.* What do you use it for?
2. What are the vulnerabilities associated with radios? *Note to interviewer. Just looking for demonstrated understanding of radio vulnerabilities.*
Section 9: Fax
1. What percentage of faxes you send or receive are transmitted over non-secure lines?
2. Do you know how to get access to a secure fax? GYes or GNo
Section 10: Other communications
1. Are there any other forms of communication that you use? GYes or GNo If yes, describe.
Section 11: Vulnerabilities *Note to interviewer. The objective is to understand the potential vulnerabilities within your organization.*
1. How could an adversary get access to information you are trying to protect? (other than communications vulnerabilities already discussed)
2. Can you think of anything we do that would give an adversary clues about where to find critical information? If so, what would it be? *Note to interviewer. You may need to provide examples such as, mass leave cancellation, a rise in posted Force Protection level, extended hours of support functions, etc.*
3. To your knowledge, are there known exploitations associated with any of the systems you are using?
Section 12: Training
1. What training have you received on the security of these communications systems? *Note to interviewer. You should reference the systems discussed earlier in this interview.*
2. Please explain what FOUO is and are there any special handling or destruction requirements?

Attachment 6

SAMPLE OPSEC SURVEY REPORT FORMAT

TABLE OF CONTENTS

Cover sheet (to be developed with organization)

EXECUTIVE SUMMARY

Who we are?

What we did?

What we learned?

<u>INTRODUCTION</u>

Background

Survey objective

What was the survey objective?

Was it to solve a known problem or was it to determine if there is a problem?

Survey constraints, limitations and boundaries

How was the survey bound so that it was manageable?

Did the resources exist to do the survey?

Where did the resources come from?

d. What was the urgency for the survey, if any?

<u>Survey Methodology</u>

Who were the key players in the sponsoring organization?

What type of support was required, i.e., red team, monitoring, etc.?

How was the OPSEC methodology applied?

Looking at the activity from Outside the box

Looking through the Eyes of an adversary

Putting the Puzzle together

THREAT SUMMARY

The Adversary Strategy
Who are they?
What are their goals or objectives?
What information do they need to meet their goals or objectives?
How would the adversary go about collecting the information needed?
What are their collection capabilities and limitations?

B. Possible Adversaries
International or domestic terrorists
2. Nation States
3. Countries

Threat Information
Unclassified Source
Classified If applicable

CRITICAL INFORMATION
Unit's
HHQ or Exercise/Operation Authority

OBSERVATIONS, DISCUSSIONS AND RECOMMENDATIONS
A. Critical information
B. Security
C. Communications
D. Operations
E. Public affairs
F. OPSEC awareness
G. Planning phase
H. Intelligence
I . Future exercises

CONCLUSIONS

Annex A—Forms

Annex B—Open Source Information

Attachment 7

VULNERABILITY REPORTING

1. General. The procedures below will be used to report or nominate an OPSEC vulnerability (see Para **2.2.1.** for vulnerability criteria) to the Air Force IO Threat Analysis Center OPSEC Section who will make fused reports available to MAJCOM OPSEC PMs and other entities as necessary.

2. On SIPRNET, go to the following URL

http://www.aia.af.smil.mil/products/database/DCIFusion/OPSECForm.cfm?state=nominateadd

This will take you to the IO Threat Analysis Center Status Board. Using the entry blocks and pull down menus enter the vulnerability or event you are reporting.

- Click on Nominate new Event
- Click on Nominate new OPSEC event (vulnerability)
- Fill out form
- Click on submit

3. This sends a notice to the IO Threat Analysis Center OPSEC section via e-mail that a vulnerability has been nominated. If the team accepts the nomination as a vulnerability, the vulnerability will be placed in the IO Threat Analysis Center Status Board database, if not accepted, a notice is sent to the nominator that it was not accepted along with a brief explanation. For assistance, contact the IO Threat Analysis Center at DSN 969-2191.